S. Hrg. 117–62

ADDRESSING EMERGING CYBERSECURITY THREATS TO STATE AND LOCAL GOVERNMENT

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JUNE 17, 2021

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
45–441 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
PAMELA THIESSEN, *Minority Staff Director*
ANDREW DOCKHAM, *Minority Chief Counsel and Deputy Staff Director*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

MAGGIE HASSAN, New Hampshire, *Chairman*

KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
JON OSSOFF, Georgia

RAND PAUL, Kentucky
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

JASON YANUSSI, *Staff Director*
PETER SU, *Fellow*
GREG MCNEILL, *Minority Staff Director*
ADAM SALMON, *Minority Research Assistant*
KATE KIELCESKI, *Chief Clerk*

CONTENTS

WITNESSES

THURSDAY, JUNE 17, 2021

ALPHABETICAL LIST OF WITNESSES

APPENDIX

ADDRESSING EMERGING CYBERSECURITY THREATS TO STATE AND LOCAL GOVERNMENT

THURSDAY, JUNE 17, 2021

U.S. SENATE,
SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT,
OF THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:15 a.m. via Webex and in room 342, Dirksen Senate Office Building, Hon. Maggie Hassan, Chairman of the Subcommittee, presiding.

Present: Senators Hassan, Sinema, Rosen, Ossoff, Paul, Scott, and Hawley.

OPENING STATEMENT OF SENATOR HASSAN[1]

Senator HASSAN. The hearing will now come to order. Good morning. The Subcommittee on Emerging Threats and Spending Oversight (ETSO) convenes today's hearing to discuss the threats to State and local entities from cyberattacks and the consequences of those attacks on national security, the economy, and the lives of our citizens. We will discuss what State and local entities need in order to be able to effectively respond to cyber threats, and how the Federal Government can best support State and local authorities as they work to combat the growing wave of cyberattacks.

While the SolarWinds, Colonial Pipeline, and JBS meatpacking cyberattacks rightly received a lot of attention in recent months, State, local, and Tribal entities have also faced serious cyberattacks that can cripple services for citizens and decimate local budgets.

The cybersecurity firm, Emsisoft, estimated that the total cost of publicly known ransomware attacks on State and local governments in 2020, including cost to restore functionality and services, was nearly $1 billion. A report from cybersecurity firm, BlueVoyant, found that there was a 50 percent increase in the number of cyberattacks against State and local entities from 2017 to 2019. At the same time, the average ransom demanded in these attacks increased 10 times, and the average cost to taxpayers to clean up after a single cyberattack rose to the millions of dollars.

Today's hearing sheds a light on the impact of attacks like the one we saw on the Sunapee School District in my home State of

[1] The prepared statement of Senator Hassan appears in the Appendix on page 31.

New Hampshire, which is represented here today by Superintendent Russell Holden. Luckily for the Sunapee community, the district had a plan in place, including a separate backup system, so it was able to resume operations soon after the attack was discovered, without paying ransom. I thank you, Superintendent Holden for your leadership on cybersecurity for school districts.

Amid the coronavirus disease 2019 (COVID–19) pandemic, we have also seen more than ever the importance of shoring up our cybersecurity. State and local agencies depend on digital delivery of services to Americans, and many State and local employees are also connecting to central networks from home in order to do their work remotely. More investment at all levels of government is needed to strengthen cyber defenses.

A 2020 survey of State chief information security officers (CISOs) found that most States only spend 1 to 3 percent of their overall information technology (IT) budgets on cybersecurity, compared to about 16 percent for Federal agencies, and many local governments, with their smaller budgets, are even worse off. Cybersecurity risks will continue to rise if State and local entities are not able to strengthen their cyber resilience.

I am working across the aisle to help State and local officials address cyber threats and increase information-sharing at the Federal, State, and local level. I am pleased that the most recent National Defense Authorization Act (NDAA) included my provision to provide each State with a federally funded cybersecurity coordinator. These coordinators will provide each State and local governments within them with a local contact who can provide support and technical knowledge, and act as a bridge to the Federal Government. I was very happy to recently learn that New Hampshire's coordinator came on board in the last week.

In addition, in this Congress I introduced a bipartisan bill with Senator Cornyn to better enable the National Guard to support State and local government cybersecurity. But we need to do more. That is why I am also working with my fellow Senators to craft a dedicated cybersecurity grant program for State and local governments.

I am excited to discuss these ideas and more with our five insightful witnesses today. Four of them represent a State, a county, a city, and a school district, and can help us better understand the unique environment that each have to operate within. They can also help us better understand which types of Federal support may be the most effective. The fifth witness is an expert in Federal cybersecurity policy and notably a former senior staffer for the Homeland Security and Governmental Affairs Committee (HSGAC). To all of our witnesses, I appreciate your willingness to testify. I want to thank you all for the role you play in helping to keep all of us safe, and I look forward to learning from you today.

With that I will now recognize Ranking Member Paul for his opening remarks.

OPENING STATEMENT OF SENATOR PAUL[1]

Senator PAUL. Thank you, Chair Hassan, and thank you to our panelists today for your time. I look forward to hearing from each of you.

I would like to begin my remarks with an observation, which is that the recent wave of ransomware attacks seems to have broken through into the public consciousness. I traveled to my home State of Kentucky recently, and was asked more questions about cybersecurity in those 10 days or so than in the previous 10 years. Of course, we as policymakers have been concerned about this malicious activity for some time, and at the Chair's request the Subcommittee held a hearing on this last December, and I am glad that we are still continuing to look at this issue.

From what I saw and heard from the people I represent, there is now a much more widespread appreciation for how disruptive these attacks can potentially be. Obviously, the Colonial Pipeline interruption and the spectre of gas shortages was a major concern. The Kentuckians I spoke to were also concerned about the ransomware attacks affecting North American meatpacking facilities owned by JBS, which may not have received quite as many headlines as the pipeline but which was also alarming.

Clearly we have a problem on our hands. The nation must be able to secure its food supply and deliver fuel where it is needed. Recent cyberattacks have also targeted hospitals, school systems, water systems, and other essential services.

How can we combat this? As the old saying goes, an ounce of prevention is worth a pound of cure. Cybersecurity must be prioritized in the same way that any other essential services are prioritized. As we will hear, recovering from cyber events such as ransomware attacks and data breaches, is several orders of magnitude more costly than what it takes to implement and maintain good cybersecurity practices on the front end.

Finally, I believe Congress needs to make sure that the Federal Government's role in detecting and responding to cyberattacks is limited and clearly defined, and that Federal cybersecurity personnel are focused, first and foremost, on the security of Federal information networks. The government can and should share information on threats and best practices with the private sector, State, local, Tribal, and territorial (SLTT) authorities. However, Congress must keep critical infrastructure operators and State, local, Tribal, and territorial in the proverbial driver's seat. One size fits all is not always the answer. Centralization is also not always the answer to cybersecurity.

I am particularly worried about a proposal that recently passed the House of Representatives which would create a new, multibillion-dollar grant program to subsidize State and local cybersecurity. The Washington solution seems to be throw money at every problem, with the result being a $28 trillion national debt.

As Americans, we face cybersecurity concerns that involve the availability of gasoline, the food supply, the electric grid, water, sanitation systems, and our communication networks. Some of these are the very fundamental building blocks of our society.

---

[1] The prepared statement of Senator Paul appears in the Appendix on page 33.

I look forward to the conversation, and I think we can all be open to what the solutions are, but I think we also need to be conscious of the fact that many of these things can be done, and are being done, in the private sector.

Thank you.

Senator HASSAN. Thank you, Ranking Member Paul.

It is the practice of the Homeland Security and Governmental Affairs Committee to swear in witnesses. Mr. Lips, if you could please stand, and all the witnesses who are joining us virtually could stand as well, and please raise your right hand.

Do you swear that the testimony you give before this Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Ms. HUEY. I do.

Mr. LIPS. I do.

Mr. WHITLEY. I do.

Mr. SCHEWEL. I do.

Mr. HOLDEN. I do.

Senator HASSAN. Thank you. Please be seated.

Our first witness today is Ms. Karen Huey, Assistant Director of the Ohio Department of Public Safety. As Assistant Director, Ms. Huey manages the department's six divisions, including Ohio Emergency Management and Ohio Homeland Security. Ms. Huey was previously the Assistant Superintendent of the Ohio Bureau of Criminal Investigations, and she has nearly 25 years of experience in State government. Ms. Huey also currently serves as the homeland security advisor to Ohio Governor Mike DeWine.

Welcome, Ms. Huey. You are recognized for your opening statement.

TESTIMONY OF KAREN J. HUEY,[1] ASSISTANT DIRECTOR, OHIO DEPARTMENT OF PUBLIC SAFETY

Ms. HUEY. Good morning. Chair Hassan, Ranking Member Paul, and Members of the Subcommittee, we appreciate the opportunity to share Ohio's specific concerns and information with you this morning. The topic of today's hearing is of great importance, and although I speak with you today from the State of Ohio, I know many of my colleagues from across the country would echo these comments.

Today I would like to share our concern that a small carve-out for cybersecurity in the current Homeland Security funding does not meet the needs of our State and local governments. The current challenge of cyberattacks, as the Federal Bureau of Investigation (FBI) Director Wray recently said, is equal to the challenge we faced by the September 11th terrorist attack.

Preventing cyberattacks takes dedicated resources, coordinated strategies, and local commitment. Ohio is investing in and making strides in our efforts to strengthen cybersecurity. The Ohio National Guard has taken the lead and brought together more than 30 public, private, military, and educational organizations to form the Ohio Cyber Collaboration Committee (OC3). Its mission is to develop a stronger cybersecurity infrastructure and workforce.

[1] The prepared statement of Ms. Huey appears in the Appendix on page 35.

Two major accomplishments of the OC3 are the Cyber Range Institute and the Ohio Cyber Reserve. As the Subcommittee is aware, States have been receiving Homeland Security Grant funding since 9/11. It has allowed us to build fusion centers, harden targets, identify critical infrastructure, and form relationships across sectors that never worked together before.

A great example of this occurred last week in Ohio. Ohio Homeland Security was alerted by a Federal Department of Homeland Security (DHS) intelligence officer who shared information about two Chinese video surveillance companies whose products have been banned by the Federal Government since 2018. Despite that Federal ban, dozens of these systems were purchased in Ohio, including some school districts and at least one hospital.

Ohio Homeland Security immediately distributed a situational awareness bulletin to alert those Ohio entities that these companies are likely providing U.S. customer data to the Chinese government for espionage and surveillance operations. Almost immediately we started receiving concerned calls from Ohio entities that had purchased these products. We were able to provide high-level technical mitigation information and CISA personnel are working on a more detailed risk management solution.

With the inclusion of cyber as a priority in the Homeland Security Grant, Ohio's local governments are struggling to address traditional preparedness needs while also prioritizing cyber projects. As the seventh-largest State, with a population of over 11 million, Ohio currently receives $6.7 million in Homeland Security funding. The current carve-out for cybersecurity is less than $340,000. I would assert that continued use of a small portion of Homeland Security Grant dollars both takes away from the needs of the traditional Homeland Security efforts and minimizes the importance of cybersecurity that we are talking about today.

We would urge Congress to consider a dedicated grant program that will enhance Ohio's and other States' ability to focus on cybersecurity capabilities. We would focus on three main areas for dedicated funding. The State would share industry standards with its local governments and small businesses; the State would also offer assessments of current systems to identify gaps and direct local governments to resources. We would provide education and training that includes cyber exercises, end user training, and resources and guidance documents.

The State would make improvements to existing secure communication platforms that would be used to gather and disseminate important, timely cyber threat information to our trusted partners.

The last piece I would mention, if there is dedicated funding, we would like to see that future funding require a condition that recipients share indicators of compromise and intrusion with the State in a confidential manner. Adding a requirement of after-action reporting will allow us to learn from and be better prepared for incidents in the future.

In closing, many States like Ohio recognize the importance of responding to cyber incidents and building a level of preparedness with our local governments. Our hope is that a dedicated cyber grant program will help ensure that we remain prepared for both

the traditional terrorist event and the cyber threat, without having to choose between the two.

We appreciate the Subcommittee's commitment to addressing cybersecurity. On behalf of the Ohio Department of Public Safety, thank you for the invitation to testify.

Senator HASSAN. Thank you very much, Ms. Huey, for that excellent testimony.

We now turn to our second witness, Judge Glen Whitley, County Judge for Tarrant County in Texas. Judge Whitley has served as Tarrant County Judge since 2007, and previously served as Tarrant County Commissioner since 1997. Judge Whitley presides over the Tarrant County Commissioners Court and provides leadership on issues related to policy and county services for the 15th-largest county in the United States. He was also a board member of the National Association of Counties and one of its past presidents. As County Judge, Judge Whitley also serves as the head of Emergency Management for Tarrant County.

Welcome, Judge Whitley. You are recognized for your opening statement.

TESTIMONY OF THE HONORABLE B. GLEN WHITLEY,[1] COUNTY JUDGE, TARRANT COUNTY, TEXAS

Judge WHITLEY. Thank you, Chairwoman Hassan, Ranking Member Paul, and Members of the Subcommittee. My name is Glen Whitley and I serve as County Judge for Tarrant County, Texas. I also serve on the Board of Directors for the National Association of Counties, and it is an honor to participate in today's hearing.

In just the past year, we have seen several cyberattacks cause major disruptions across the United States. These attacks all demonstrate the vulnerability of our nation's cyber infrastructure. At a local level, Pinellas County, Florida recently experienced an attack on their water treatment facility that allowed hackers to manipulate their water supply. As county reliance on technology increases, these attacks will likely increase as well.

To better understand how local government can respond to cyber threats, it is important to start with an understanding of the underlying challenges to the local revenues and resources. General revenue from local property taxes are the backbone of county funding, because they are not restricted to a particular activity. Currently, though, 43 States are imposing some type of limitation on a county's ability to increase local taxes.

Restrictions on Federal and State resources also remain a challenge. Locally collected general revenues are not restricted to a particular activity. Unfortunately, about 93 percent of State and Federal funding used by county governments is restricted to a specific function. Matching requirements for Federal grant and loan programs also make leveraging Federal resources impossible for many counties.

We applaud Congress for providing $61.5 billion to county governments in the American Rescue Plan (ARP) Act. However, local governments are prohibited from using these dollars as a non-Fed-

[1] The prepared statement of Judge Whitley appears in the Appendix on page 40.

eral match for grant and local programs. Without relieving these pressures, counties will struggle to invest in the cybersecurity infrastructure they need.

Collectively, counties own or operate thousands of hospitals, public health departments, water and waste management centers, jails, and emergency operations centers, all of which create significant cyber vulnerabilities. Without robust and reliable funding, these local assets expose our communities and these critical programs and services.

It is important to note that cybersecurity needs are not only driven by exposures and vulnerabilities but also by the need to meet national standards. In Tarrant County, we adhere to the four principles of the NIST Cybersecurity Framework. Achieving and maintaining the core principles require an Information Security Program that includes policies, procedures, and resources. While policies and procedures can be downloaded and customized, resources require continuous funding.

More generally speaking, county cyber resources are typically directed to three main areas: education, infrastructure, and preparedness.

An organization's greatest cyber weakness is the end user or the employee. A recent cybersecurity survey found that 70 percent of the employees polled said they had recently received training from their employers, yet 61 percent failed their basic quiz.

One of the best cybersecurity practices is the implementation of multi-factor authentication. Counties must also update and replace network devices and vet cloud software and supply chains, all of which require time, money, and skilled personnel.

Preparedness depends on the county's ability to effectively monitor cyber threats. Counties must develop, test, and retest security policies and incident procedures or hire trusted, expensive third-party contractors.

As the Committee considers how to best allocate cybersecurity investments, it is imperative that Federal resources reach their intended targets as quickly as possible. We applaud Chairwoman Hassan's work to provide local governments with reliable and flexible cybersecurity resources in the State and Local Cybersecurity Improvement Act.

In closing, counties need a strong Federal partner that can provide direct and flexible resources that allow local governments to adopt resources to meet the unique needs of their communities. This is especially true for cybersecurity resources. Again, local governments own and operate some of our nation's most critical infrastructure.

Thank you for allowing me to be here today.

Senator HASSAN. Thank you very much, Judge. Now we will move on to our third witness, Mayor Steve Schewel of Durham, North Carolina. Mayor Schewel has served as mayor since 2017, and previously served 6 years on the Durham City Council and as Vice Chair of the Durham Public School Board. He is a long-time member of the Durham community and a visiting professor at the Sanford School of Public Policy at Duke.

Welcome, Mayor Schewel. You are recognized for your opening statement.

TESTIMONY OF THE HONORABLE STEPHEN M. SCHEWEL,[1] MAYOR, CITY OF DURHAM, NORTH CAROLINA

Mr. SCHEWEL. Thank you very much, Chair Hassan, Ranking Member Paul, and Members of the Subcommittee. On behalf of the city of Durham and the National League of Cities, thank you for convening this important discussion today. I am Steve Schewel, mayor of the great city of Durham, North Carolina, home to more than 280,000 residents, and home to Duke University, North Carolina Central University, and North Carolina's Research Triangle region.

Cybersecurity is a top priority for the city of Durham. Our city has experienced recent cyberattacks, including a ransomware attack in March 2020, at the start of the COVID–19 pandemic. During that attack, our city was fortunate to maintain functioning of critical systems, including our 911 call center, and we did not pay a ransom. This was due to the city's prioritization of cybersecurity planning and preparation in the wake of an extremely disruptive attack on Durham Public Schools in 2009, and a smaller malware attack on city networks in 2018. Our city was able to resume full network functioning in less than a week after the attack. This was thanks to our advanced planning, our robust system of cloud backups for city data, and our partnerships with our vendors, the FBI, and the North Carolina National Guard.

However, this preparation is costly for our city, and too many cities, towns, and villages are not as well prepared as the city of Durham. It is not a matter of if another devastating attack will paralyze critical municipal networks and infrastructure, but when.

The United States has thousands of municipal governments which operate water systems, gas and electric utilities, 911 answering centers, transportation systems, and countless other critical services. Most of these municipal governments are small with limited budgets. Cybersecurity is competing directly with direct services such as providing safe, quality drinking water, maintaining infrastructure, such as replacing 100-year-old water pipes or repaving pothole-ridden streets, and employing first responders to keep our communities safe.

Meanwhile, cybersecurity has become more complicated and expensive every year. Criminal organizations, including State-backed criminals, continue to develop sophisticated methods for penetrating public networks and disrupting city functions. Even small-town networks are attractive targets for these bad actors, and we can no longer rely on security through obscurity.

Relatively basic steps, such as implementing multi-factor authentication, conducting cyber hygiene training for city staff and elected leaders, and maintaining up-to-date hardware and software can be very costly for a city. Many municipalities, including the vast majority of smaller towns, lack sufficient budget for cybersecurity and outsource most IT functions. We depend on our partnerships with vendors, the State, and Federal agencies to keep our networks safe and recover from an attack.

Congress has the opportunity to bolster these partnerships and provide cities, towns, and villages with new resources to strengthen

[1] The prepared statement of Mr. Schewel appears in the Appendix on page 47.

our collective security posture. We recommend three principles for any new cybersecurity program in support of State and local governments.

First, Congress should provide sustainable new funding without cannibalizing existing public safety grant programs. Cybersecurity measures are ongoing expenses, and while a one-time grant will help get some efforts off the ground, network monitoring, training, and upkeep must be budgeted for every year.

Second, Congress should prioritize intergovernmental partnership. Closer collaboration between city, county, State, and Federal agencies on things like planning, procurement, training, and incident response will help reduce the impact of attacks experienced by local governments and the time needed to recover.

Finally, Congress must be careful not to impose a one-size-fits-all solution on local governments. Cities and towns come in all shapes and sizes. Some would benefit most from a direct grant, while smaller communities may prefer that Federal support be administered by the State.

Again, I thank you so much for your attention on this important and timely issue, and I look forward to your questions. Thank you very much.

Senator HASSAN. Thank you so much, Mayor. I really appreciate the testimony.

Now we will go to our fourth witness today, Superintendent Russ Holden, of Sunapee School District in my home State of New Hampshire. Superintendent Holden has worked as a public school administrator in New Hampshire for the last 26 years. As superintendent, he is responsible for evaluation of all administrators and directors for the school district, and for managing all Federal and State grants. He is also the Vice President of the New Hampshire School Administrators Association, where he serves as the chair of the Policy Committee.

Welcome, Superintendent Holden. I am looking forward to when I can see you again in person, and you are recognized for your opening statement.

TESTIMONY OF RUSSELL E. HOLDEN,[1] SUPERINTENDENT, SUNAPEE SCHOOL DISTRICT, NEW HAMPSHIRE

Mr. HOLDEN. Thank you, Senator Hassan, and thank you to the Subcommittee. I appreciate the opportunity to speak to you today, and I will keep my comments brief because you have my written testimony.

In October 2019, we came in after a weekend and found out that our data had been held for ransom, and everything that we had in our school district was kept from us. Sunapee is a small district in the western part of the State. We have about 430 students, Pre-K through 12, and about 120 faculty members. Our IT department consists of 1.3 people. We are basically the biggest employer in our town.

Upon finding that we were held for ransom we quickly notified our local police and State police and our insurance carrier. Unfortunately, neither our local police or State police at the time really did

[1] The prepared statement of Mr. Holden appears in the Appendix on page 93.

not have much assistance that they could give us, and the assistance really came from our insurance carrier, putting us in touch with professionals and lawyers that had dealt with these situations in the past.

Fortunately enough we had a backup system in place, and the interesting piece about our backup system was prior to this incident, a week prior, we realized that our backup system had failed, and if we had not recognized that at that time and instituted a new backup system, we would have lost information going back 6 months. With the backup system in place, we were able to recover our data, without paying the ransom.

The long and short, we accumulated fees and materials totaling more than $40,000, and it took over 9 days for our IT department to get us back up and running fully.

While 9 days may not seem like a lot, fortunately technology has really integrated itself into education, and education into technology, and really having our teachers pivot very quickly and go back to some of the older ways that we learned how to educate our students, using more paper, pencil, and traditional materials. Our ability to do that really allowed us to continue and not to have to cancel school and allowed us to stay in school and educate our children, which is our primary task.

We have about a $12.5 million budget here in Sunapee, and about $500,000 of that is dedicated to technology. After going through this ransom situation, we invested last year $10,000 to go through an audit that looked at our entire security system. Through that audit, much of what other folks are presenting here today have said, we found out that we quickly needed to put things in place, like disaster recovery plans, business continuity plans, backup systems particularly that can be held offsite or in the cloud, enabled multi-factor authentication, and train ourselves in phishing drills and help educate staff and students on outside threats, including looking at dry sprinkler systems within our IT server closets.

Again, as I mentioned, our IT department consists of 1.3 people. Going through that audit process we quickly realized that we were completely understaffed, but hiring a new person would add at least one percent to our overall budget.

I am also a member of the American Association of School Administrators (AASA), and was completing my national certification program in February 2020, and I had the opportunity to share this incident with 20 colleagues from across our country, from States of California, Pennsylvania, Illinois, and Virginia. At that point in time, little old Sunapee represented the smallest school district in the cohort, Bakersfield, California, with 260,000 students. When speaking to my colleagues they all said, "We are not prepared to know what we would be able to recover the data potentially that was lost and get ourselves back on our feet."

I would echo again what some of the other folks said here today. I think there are ways that we can look at Federal monies, either using Homeland Security or Title IV monies that are given to school districts, try to free up some of the restraints and constrictions that are on those so they can be sent to help us look at more appropriate ways and more sufficient ways to help educate our stu-

dents and staff and community of these security and ransom attacks.

I would again thank the Senate Subcommittee and Senator Hassan for representing the State of New Hampshire and by continuing to bring this topic forward. Thank you.

Senator HASSAN. Thank you, Superintendent Holden.

Now I am going to turn to our final witness who is joining us in person in the hearing room today, Mr. Dan Lips, Vice President for National Security and Government Oversight at the Lincoln Network. At the Lincoln Network, Mr. Lips focuses on research and advocacy between technology, government oversight, and national security.

Mr. Lips began his career as an intelligence analyst with the FBI. He also served as a staff member of the Senate Homeland Security and Governmental Affairs Committee, where he worked on cybersecurity policy and served as Homeland Security Policy Director.

Welcome, Mr. Lips. You are recognized for your opening statement.

TESTIMONY OF DAN LIPS,[1] VICE PRESIDENT FOR NATIONAL SECURITY AND GOVERNMENT OVERSIGHT, LINCOLN NETWORK

Mr. LIPS. Thank you. Good morning, Chairwoman Hassan, Ranking Member Paul. Thank you for the opportunity to testify.

My name is Dan Lips. I am the Vice President for National Security and Government Oversight at Lincoln Network. As a former HSGAC staffer, it is a real honor to testify. I sincerely respect the Members and staff of this Committee and the work that is done in this hearing room.

We have heard sobering testimony this morning. State and local governments face growing cyber threats that warrant a proactive response by the Federal Government. But Congress should be thoughtful about the resources currently available to spend on cybersecurity. The Government Accountability Office (GAO) has warned that the Nation is on an unsustainable fiscal path, including that the growing Federal debt could cause a large drop in the value of the dollar and limit Congress' ability to respond to future emergencies.

With that context, what should Congress and the Committee do to help State and local governments manage growing cyber risks? I will offer four recommendations.

First, Congress should streamline Federal rules to reduce State governments' compliance costs to allow more resources to be spent on improving security. For years, the National Association of State CIOs and the National Governors Association (NGA) have urged Congress and the White House to harmonize agencies' information security rules, which are often contradictory and duplicative.

In 2018, the Oklahoma State CIO testified that his office spent 10,000 personnel hours complying with Federal rules and audits. That is a year's worth of work for five employees, full-time, and that is time that could be spent otherwise on improving security.

[1] The prepared statement of Mr. Lips appear in the Appenidx on page 95.

GAO has reported that the Office of Management and Budget (OMB) has issued guidance to agencies, encouraging them to harmonize rules, but did not require them to do so. Congress and the Committee could pass legislation to require agencies to harmonize Federal rules and audits to fix this problem.

Second, Congress should prioritize cybersecurity and existing Homeland Security Grant programs, and States should use available Federal funds for cybersecurity. I appreciate that Members of Congress have proposed creating a new cybersecurity grant program, but DHS, through the Federal Emergency Management Agency (FEMA), already awards more than $1 billion in annual Homeland Security Grants. Secretary Mayorkas recently announced the Department would require grant recipients to spend 7.5 percent of grants on cybersecurity. Congress could further increase that amount.

But States and localities do not need to wait on Congress. They already have billions in unspent DHS grants and other funds that could be used for cybersecurity. According to OMB, States had not spent 50 percent of the Homeland Security Grants that have been awarded since 2015, and $2.7 billion was still available as of 2020. After receiving $340 billion in additional funds through the American Rescue Plan, State and local governments should have resources to improve cybersecurity.

Third, the Federal Government should share meaningful threat information and security recommendations to help organizations manage cyber risks. Over the past decade, Congress has passed bipartisan laws to establish Federal programs to facilitate information sharing. But watchdogs have identified limitations and opportunities to improve DHS' information-sharing programs. Congress should press the Department to implement these recommendations.

The Federal Government should also better leverage its expertise to help State and local governments and other partners implement best practices. For example, NIST provides valuable guidance through its Cybersecurity Framework. But the framework includes a checklist of more than 100 recommendations, which are difficult for many organizations to fully implement.

The White House recently issued a memo to American companies with five specific recommendations to prevent and prepare for ransomware attacks. This is exactly the kind of specific and focused security recommendations that are needed to help organizations manage cyber risk.

Fourth, Congress and the Subcommittee should conduct a strategic review of cyber threats and assess current and future resource needs to manage long-term risks. The intelligence community (IC) recently assessed that technological innovations will likely result in increasing competition in the cyber domain in the future. Congress should forecast what resources are needed moving forward.

President Biden proposed spending $9.4 billion on Federal civilian agency cyber programs in his recent budget, or a 14 percent increase. In comparison, he proposed spending $750 billion on national defense. Congress should consider whether these resource allocations are appropriately balanced to address current and future threats.

There is also significant waste in the Federal budget, such as the $75 billion that is lost annually on improper payments, according to GAO, which is much larger than what Congress currently spends on cybersecurity. Given the Subcommittee's mandate, you are uniquely positioned to review and forecast what Federal spending resources are needed to counter emerging threats.

Again, thank you for the opportunity to testify. I look forward to your questions.

Senator HASSAN. Thank you so much, Mr. Lips, for that testimony. We now will turn to our rounds of questions. I will start and then move to Ranking Member Paul.

To Ms. Huey and Mayor Schewel, a functioning government depends on functioning computer systems, and we have seen this more than ever during the COVID–19 pandemic. A cyberattack on a State or local entity can easily disrupt services to people or hamper the functioning of a government entity.

Ms. Huey and Mayor Schewel, can you outline what the consequences might be of a cyberattack on your organization? What data do you have that would potentially be at risk? What critical services might be disrupted? We will start with you, Ms. Huey.

Ms. HUEY. Thank you. At the Ohio Department of Public Safety we have, obviously, several large systems under the Bureau of Motor Vehicles. You can picture the driver's license, vehicle registration, all of that citizen data would be impacted if we sustained an attack.

In addition to that, we also operate the Law Enforcement Automated Data System (LEADS), and this is the system that collects all local law enforcement arrests, criminal justice information. It is shared throughout the State, and it is also shared with our Federal partners.

We feel that we have very robust security measures around this, but it obviously would be a very big blow to public safety at the State, local, and Federal level if something were to happen to LEADS.

Finally, we use a confidential information management system for Homeland Security to communicate with our trusted partners, and we would hate to see something happen to that, that would disrupt services to our citizens.

Senator HASSAN. Thank you. Mayor Schewel.

Mr. SCHEWEL. Thank you very much. Our 911 center is absolutely crucial. We receive 300,000 calls a year to our 911 center, and any disruption in that service would be a terrible blow to our residents. In addition, we operate a water system that has 90,000 customers, and 25 million gallons a day of water. Any disruption to that would also be an absolutely terrible blow.

There are other systems as well, but I think those are the two most crucial systems that we operate that could potentially be devastatingly impacted by a cyberattack.

Senator HASSAN. Thank you very much, Mr. Mayor.

The next question is for Superintendent Holden, again Mayor Schewel, and Judge Whitley. Superintendent Holden, Mayor Schewel, and Judge Whitley, you all experienced a cyberattack within the last few years. Would each of you highlight the actions your organizations took to limit the impact of these attacks on your

operations? What can other local entities learn from your example? We will start with you, Superintendent Holden.

Mr. HOLDEN. Thank you, Senator. I think first and foremost I have to say what will win at that is your personnel. Having dedicated IT professionals that are willing to spend the time and energy to continue to be up to date and put not only systems in place but to stay current on what is going on in the world around us, when it comes to these matters. Making sure that the appropriate training is in place, making sure that you have the proper amount and rightly placed backup systems I think are also a key part of ensuring these things did not happen and preventing them from happening.

Again, the last piece I think, again going back to the training, we are only going to be as good as our users. At Sunapee we have about 650 end users, and that is what it is going to come down to, how well we can train our end users.

Senator HASSAN. Thank you. Mayor Schewel.

Mr. SCHEWEL. We had a terrible attack, devastating attack on Durham Public Schools network in 2009, and after that we established plans and policies and procedures to ensure that the city would not experience a similar costly disruption. We established a comprehensive plan and budget for improvements over time. We established working relationships with the FBI, State leaders in North Carolina, the Multistate Information Sharing and Analysis Center, and these plans were tested in 2018, when a second attack occurred, this time impacting the city's fleet vehicle network.

We established a war room, once we were attacked in 2020, with representatives from our staff, contractors, other governmental partners, including the North Carolina National Guard, to respond to and recover from the attack. I will say this was made particularly challenging, because we were navigating this with the new social distancing protocols that we needed in March 2020. We were fortunate that we had regular backups from all city data, and that was crucial.

Senator HASSAN. Thank you. Judge Whitley?

Judge WHITLEY. Again, I think the backups, we have heard this mentioned a couple of times today already. That is very important. We have a playbook that we look at, that helps us to identify, contain, eradicate, and really begin the recovery from that. Then we go back to the education process of trying to make sure folks understand and learn from any issues that we have, and we looked at that. We always are having tabletop discussions and exercises, from that standpoint.

Senator HASSAN. Thank you very much, sir.

One more question before I turn to the Ranking Member. To Superintendent Holden and Judge Whitley, good cybersecurity requires up-front investment, but State and local entities often have limited resources and they have to balance competing priorities. A Federal grant program that focuses on cybersecurity can help relieve State and local resource constraints and increase investment in cybersecurity.

Superintendent Holden and Judge Whitley, what are the resource constraints that you face when deciding how much to invest in cybersecurity, and are there improvements to cybersecurity resil-

iency that you would make if given a reasonable amount of additional resources?

We will start with you, Superintendent Holden.

Mr. HOLDEN. Thanks, Senator. The answer to your last question is yes, absolutely. Our ability to improve our resources greatly has an impact on our financial situation. One of the first things I think that comes to mind for us would be a dual authentication, and that would be allowing you to sign in not only on a computer but on another device. That would us having another device for every person in our district, so basically doubling what it is that we currently have in the public sector. That would have a tremendous impact on our budget. Thank you.

Senator HASSAN. Thank you. Judge Whitley.

Judge WHITLEY. I think as we look through there is always the balancing of how do we spend our dollars, and more often than not now what we are seeing are attempts, sometimes from the State level, to limit the amount of dollars that we can raise and to be able to allocate. Flexibility is key as far as I am concerned.

One of our witnesses before talked about how different we are among counties, among States, among cities and towns. The flexibility really allows the local area to assess the threats that they feel most strongly about and to be able to allocate that, among personnel or among different programs.

Senator HASSAN. Thank you. I will now turn to the Ranking Member for his round of questions.

Senator PAUL. Mr. Lips, the Chairwoman and I have been interested in duplication, and I have a bill actually to have reports on bills from the Congressional Budget Office (CBO), whether or not we already are doing through another program. You mentioned that we hand out FEMA grants that already deal with cybersecurity. In your opinion, would a new grant program just for cybersecurity be a duplication of what we are already doing through the FEMA grants?

Mr. LIPS. I believe so, particularly since cybersecurity is an allowed use of the existing FEMA grants.

Senator PAUL. I think this is an important question because money does not grow on trees. We are institutionally about $1 trillion short every year, just for Medicare, Medicaid, food stamps, and the military. We are short on the ordinary expenses, and we have been adding extraordinary expenses of trillions of dollars. Last year the deficit was over $3 trillion, likely over $3, maybe even $4 trillion this year. We have to figure out how to most wisely use our resources.

I was intrigued by your point, though, that even without legislation we are giving $1 billion a year—so we have about $5 billion over the last 5 years—and yet we have only spent a little over half of it. Has that money been given in grants and just not spent by the recipient, or it has not yet been applied for?

Mr. LIPS. My understanding is that it has been awarded, and that it is with the States, and that it could be put to use. Why States have not spent that is not fully clear to me.

Senator PAUL. All right. I think that is worth a letter, and maybe the Chair might consider that we send a letter asking if the money has been allocated, and it is for cybersecurity, asking the people

who received it to tell us why they have not used it yet or what the problem is. Maybe try to figure out what is going on with that money.

Senator HASSAN. I am certainly happy to consider that. I think this depends a lot on what the overall grant is and how much is restricted.

Senator PAUL. Our staffs can work together to figure that out. But it is also interesting that even without legislation, Secretary Mayorkas has increased the requirement from 5 percent to 7.5 percent, so that is a 50 percent increase in the funding. Instead of $5 billion it will be $7.5 billion over the next 5 years?

Mr. LIPS. My understanding is that it is actually out of that pot of funding, so out of $1 billion, 5 percent is required to be spent on cybersecurity, and he is increasing it to 7.5 percent.

Senator PAUL. OK. The whole $5 billion does not go to cybersecurity. It is 5 percent of that, and he is increasing that to 7.5 percent of that. OK, I got where we are.

But the other possibility is you could even go up even more significantly. We could either do that through legislation, we could say 20 percent of that money needs to go to cybersecurity. If we really thought cybersecurity was a pressing issue we could try to reallocate or resource that money that already exists.

Mr. LIPS. Absolutely, Senator Paul, and I think it would be wise for Congress to consider doing that. The FEMA grant programs for homeland security were expanded and created after 9/11, and the intention was for them to be risk-based and to focus on existing security threats. Twenty years later, it is clear that this has become a serious security threat and it should be prioritized. It would make a lot of sense for more of those funds to be used to address these problems.

Senator PAUL. While I think we all agree that cybersecurity is a problem, putting in perspective of our overall national security is important, when you talked about weighing how much we spend on national defense. But also there have been remarks from even folks within the military community. Admiral Mullen said, a few years ago, that the greatest threat to our national security was actually our debt.

I think we cannot, on the one hand, say we are going to throw unlimited resources. We have to be careful about where the resources are and try to redirect resources to a problem. If we think cybersecurity is a pressing issue, which it sounds like it is, let's take it from maybe less pressing issues and try to force some of the money over toward that without necessarily spending more money. I would probably support legislation if we had legislation that did what Secretary Mayorkas did. We could do it even more, figuring out what the appropriate number is. But you could take more of that $5 billion and push more toward national security simply by looking at those percentages.

I had one other question that kind of a technical question. I always ask this because I am somewhat intrigued, without being a technological or a computer expert on this. It seems like the articles that you read say most of the people get into your system through your email. Is that still true? Would half the people be getting in through email, or is that a rare way they get in?

Mr. LIPS. It is certainly one of the ways that attackers get into systems, and certainly it is encouraging to hear some of the precautions that are being taken by my fellow panelists. There is a lot that can be done to understand best practices, to improve cyber hygiene, such as not clicking on suspicious emails, and other measures to——

Senator PAUL. It would seem to me that it should not be that hard, technologically, to wall off your email, where your email has no communication and you cannot get from your email to your operating system. Can you make it a wall such that it cannot be penetrated?

Mr. LIPS. That is a good question, and I am not sure. I am encouraged by what the Biden administration recently put out as recommendations to address malware and ransomware. There are simple things that can be done, such as backing up systems, encrypting data at rest to make it less valuable to ransomware attackers. There are some relatively simple things that can be done to improve organization security posture, that should be prioritized.

Senator PAUL. Twenty years ago, as a physician, we used to back up our records every day on a floppy disk, and we would put them in a fireproof safe, in case the building burned down or in case you had an electrical surge you would not lose all your patient data. I know it would not be on a floppy disk anymore but it would seem that there would be ways to back this up on a daily basis and protect yourself. There has to be ways.

I think a lot of this stuff is not necessarily rocket science. There are available solutions out there, and I think it is important that we get that out there for folks to prevent.

The other thing I had heard a lot was that people were doing a lot more work from home. They would be working on their phone or their computer and they had not done the updates, and the updates are pretty sophisticated to protect against viruses. I am guilty of it too, not always pushing to accept the update, and maybe that has been part of the problem in the last year as well.

Mr. LIPS. Absolutely, and those were some of the recommendations, sir, that were included in the White House's recent memo to companies, to update and patch systems regularly. These are basic actions that organizations can take to improve their security.

Senator PAUL. Thank you.

Senator HASSAN. I think we are expecting Senator Ossoff shortly, but why don't I ask a question until he gets here, unless that is him.

Senator, would you like a minute? You are up, or——

OPENING STATEMENT OF SENATOR OSSOFF

Senator OSSOFF. I am ready to go.

Senator HASSAN. You are ready to go? Then I will turn the questioning over to Senator Ossoff.

Senator OSSOFF. Thank you, Madam Chair. Thank you to our panelists who are here in person and remotely. My first question is for Ms. Huey.

Ms. Huey, in March 2018, the city of Atlanta suffered a severe ransomware attack. According to Bloomberg CityLab, the hackers encrypted files, locked access to online services, blocked the city of

Atlanta from processing court cases and warrants, and demanded a $51,000 ransom. Just 2 months prior, the City Auditor's Office released a report finding that the city's information security management system, "has gaps that would prevent it from passing a certification audit," and that many information security management processes, "are ad hoc or undocumented, at least in part due to lack of resources."

Similar issues prevail across major cities. It is not unique to Atlanta. A recent study by the National Association of State Chief Information Officers found that States spend only a fraction of their IT budgets on security, between 1 percent and 3 percent, compared to about 16 percent for Federal agencies.

Given the budget constraints that States and municipalities face, what are the cybersecurity investments that, in your view, would have the biggest impact, the highest return on investment, when it comes to preventing, for example, ransomware attacks and securing State and municipal networks?

Ms. HUEY. Thank you for that question. Senator, I believe that State government has done a good job of looking at State assets and providing a level of security. Where I think dedicated cybersecurity funding that could come into the State could help us focus on local governments. As you have heard today from the other witnesses, there is a variety of levels of preparedness that local governments have been able to do with cybersecurity.

What we would hope to do, at the State level, is those standards there already identified in industry, making sure that those are communicated across the State, and then provide those assessments and those audits so that we can go out and help people identify those gaps and then identify resources for them to use.

I think this is always a combination of local, State, private investment, along with Federal dollars that will make it successful. Thank you.

Senator OSSOFF. Thank you, Ms. Huey, and, of course, we do want that strong intergovernmental communication and communication and best practices, sharing of threat information. Can you drill down in a little more detail, what do you think consistently municipal or local governments are maybe underinvesting in? What would be the best use of their limited resources? Is it data hygiene practices for personnel? Is it firewall technology? Is it supply chain checks? Is it robust patching practices, hardware, software? How should local governments deploy resources that are limited for most effect?

Ms. HUEY. I can tell you that the locals that took advantage of the 5 percent cyber set-aside, our first round of funding here in Ohio, obtained cyber risk assessments. That is what they were looking at, was looking at a contractor, and this was a little bit of a regional approach, so maybe 3, 5, 6 counties went together and were looking at doing a cyber risk assessment that would then make recommendations on hardware and the issues that you identified.

Senator OSSOFF. OK. Thank you, Ms. Huey.

Mr. Whitley, you mentioned in your testimony that lack of cybersecurity awareness, training, and implementation and best practices for employees as well as local government staff is a major im-

pediment. I believe you cite a study showing that most folks polled had been given cybersecurity training but also failed basic quizzes on the topic and best practices.

Committee-provided information indicated that recent cyberattacks in both Tarrant County and Durham, North Carolina, were the result of phishing email campaigns, where individuals are tricked into clicking links that can load malicious software.

If the Federal Government were inclined to make investments in cybersecurity training, how could we be certain those investments would have a positive impact and actually address the security challenges counties like yours are facing, and what do you believe are the best practices for not putting personnel through online presentations and then calling it job done but actually ensuring that staff understand the underlying concepts and best practices.

Judge WHITLEY. Thank you for that question. I think the best thing is to continuously test, retest, educate. A lot of time we will say, OK—in fact, we just finished a program by which everyone had to go in and do this training, and if they did not we ended up turning their systems off. I know actually five elected officials who all of a sudden looked and their screens were blank.

We have to keep pushing and pushing and pushing on the education, but even after that, sometimes testing from internally and saying, "OK, we told you about this and now all of a sudden we tried you and you still failed," that has a lasting impression on at least that employee. I think that word gets around to other folks, and they begin to realize, OK, this really can happen and I need to be a little bit more careful, because the last thing in the world you want to do is be the reason why our systems were taken over or were shut down.

It is a combination of things, but it has to be a continuous, constant reminder, and emphasizing how important it is to be careful about whatever you open and whatever websites you may go to.

Senator OSSOFF. Thank you, sir. Mr. Lips, finally, in your testimony you emphasized the need to improve information sharing about cyber threats and best practices across the Federal Government, between Federal agencies, about potential vulnerabilities in the information technology ecosystem to improve their technology acquisitions and strengthen supply chain risk management. Obviously, sharing information is good. But can you describe, in a bit more detail, the current limitations on information sharing, in particular with respect to supply chain risks?

Mr. LIPS. Thank you for the question, Senator. Over the past decade it has become clear that the Federal Government has focused increasing attention on addressing supply chain risk management. We have seen actions to ban the use of certain technologies by Federal agencies. From my perspective it seems like there is a time delay between when Federal agencies become aware of these problems and then when it reaches an understanding on Capitol Hill and then when it is implemented across the Federal Government.

In 2018, there was legislation that attempted to address this problem by creating a stronger interagency process to improve that information sharing across the Federal Government. It seems like it would be a productive next step for Federal agencies and that interagency task force to also share information and specific infor-

mation, to your point, with State governments, municipal governments, and the private sector.

One of the challenges we have seen over the years with cybersecurity best practices is that there is often long lists of information provided to organizations. Providing very specific and discrete recommendations will help organizations, particularly those with limited resources, decide how to prioritize and manage risk.

Senator OSSOFF. Making the information that is shared more actionable rather than just a bureaucratic dump of data perhaps?

Mr. LIPS. Absolutely, Senator.

Senator OSSOFF. OK. Thank you, Mr. Lips. Thank you, Madam Chair.

Senator HASSAN. Thank you, Senator Ossoff. I am going to start my second round of questioning. I think we are expecting Senator Rosen to be available relatively soon, and when she gets here let me know and we can let her jump in, and then I can finish up with additional questions.

I want to start with a question to Judge Whitley and Ms. Huey, because, again, this is a theme we are hearing, cybersecurity is a team effort. We know State and local governments often have separate structures for technology and security, but working together and sharing resources and best practices can improve the cybersecurity of all entities.

Judge Whitley and Ms. Huey, do you think States should use a committee or other structure to bring together State and local representatives to help plan and coordinate cybersecurity efforts, and if your State already has such a committee, could you please elaborate on how effective you think it is? We will start with Judge Whitley, please.

Judge WHITLEY. I do feel like it is extremely important. In this recently adjourned session of our legislature they created a committee that will go into effect on September 1st, and I think that will be very helpful. We will see how it works itself out.

I really want to say, though, it is important to get our dollars back down as much as possible to the end user. Committee is OK, but again we are very different, we are very diverse, we are a very large State, and the quicker the dollars can get from wherever they are coming, whether it be the Feds or the State, and get it down to the end user, the better off it will be.

An excellent example that I will use is the ARPA funds, which you allocated out. Counties, regardless of their size, receive the monies as direct payments.

Senator HASSAN. Right.

Judge WHITLEY. In the CARES Act, it was distributed out to the State, except for those counties and cities over 500,000. Some of that money is still sitting in the States. The quicker you can get it down to the local areas, the better off we are.

Senator HASSAN. Thank you. Ms. Huey.

Ms. HUEY. Thank you, Chair. I absolutely believe that using an advisory committee, an advisory board, made up of a combination of State and locals best help define the strategy on how to spend funding and how to address cybersecurity.

In Ohio, we have two organizations, the OC3, which I had already mentioned, which is a combination of public and private, is

always a resource for any cybersecurity decisions. They are very much focused on economic development and workforce and sort of prevention. That would be their expertise. Then we also have the Homeland Security Advisory Council, which actually advises us on how to spend the Homeland Security Grant on our strategic goals.

There are already a couple of systems in place in Ohio, and I would hope that many States have this. That would be a help with funding decisions.

Senator HASSAN. Thank you both for those answers. I am now going to ask another question of Ms. Huey and then Mayor Schewel. While the Federal Government can provide some resources and support to State and local cybersecurity efforts, we also need to encourage more State and local investment in cybersecurity, and that is a theme that we have been hearing this morning. That is why recent proposals for State and local cybersecurity grant programs have included a cost share where the grant would supplement funds already provided by the State or local entity.

However, sometimes this cost share can be a barrier to State and local entities utilizing the grant program, especially during economic downturns, especially because State and local governments have to balance their budgets.

Ms. Huey and Mayor Schewel, do you think that the Federal Government should be able to waive the cost share requirement in certain limited circumstances, and what would those circumstances be? We will start with Ms. Huey.

Ms. HUEY. Thank you for that question, and I appreciate having the cost share requirements, the match requirements. I think it is important to have skin in the game. But, if that can be done on a graduated basis so that things can get stood up and get started, and then other sources of funding can eventually supplement, I think that is a great approach.

Are there opportunities to waive that? I think that would be interesting and potentially a multi-state project or something that is a little bit broader. At that point in time if it is a waiver or maybe we could leverage private dollars for something like that, I think that would be something interesting to pursue.

Senator HASSAN. Thank you. Mayor Schewel.

Mr. SCHEWEL. Thank you very much, Senator. Durham is lucky. We are a fairly large city with really good IT staff. We have wonderful staff. But 80 percent of municipalities in the United States are small with populations below 50,000 people. Most of these municipalities have very little ability to cost share, and I think that really needs to be an important consideration.

The Public Technology Institute found that 65 percent of IT officers in municipalities felt that their cybersecurity budget was inadequate, and many of these cities are pressed in many ways, multiple needs for their budgets. Cost sharing certainly can be an impediment to have the adequate cybersecurity infrastructure that is needed.

Senator HASSAN. Thank you very much, Mr. Mayor. I now see that Senator Rosen has joined us virtually, so I will recognize her for her 7-minute round of questions.

Senator ROSEN. Thank you, Madam Chair. I appreciate that. Thank you for chairing this meeting in the absence of Senator

Peters being here on the loss of his mother. I really appreciate you stepping in, and the witnesses, of course, for being here today, because cyberattacks can be expensive, they are debilitating, especially for small governments. I am really glad that we are coming together in a bipartisan way to talk about how we are going to protect communities in this really challenging time, and it is not going to get any easier.

Elementary and secondary schools, they remain increasingly vulnerable to hostile cyber actors. Last year, the FBI warned that K–12 institutions represent an opportunistic target to hackers, and many school districts, they lack the budget and the expertise to dedicate to network integrity.

In August of last year, Clark County School District, Nevada's largest school district, and our nation's fifth-largest school district, was the victim of a ransomware attack. The hacker published documents online containing sensitive information, Social Security numbers, student names, addresses, and the like. Of course, this is absolutely unacceptable, and the Federal Government must help schools obtain the tools and resources to protect their students, their families, their teachers, educators, everyone who works there. It is something that I have raised with CISA and the Department of Education.

Mr. Holden, what more could CISA be doing to assist our elementary and secondary schools with being sure that they have some way to understand how to implement the tools and cybersecurity standards and protocols?

Mr. HOLDEN. Thank you for the question. I think really what needs to happen is there needs to be a set of standards developed. I think if either Homeland Security took a look at cybersecurity and implemented a set of standards that would then pass down to us, that we could look at at the local level, or even at the State level, to make sure that we have implemented those systems to prevent ourselves from what is out there.

I would highly recommend a set of standards that could be looked upon, and then a way for either Homeland Security or the local or State to test those systems for us, and then to identify where we may be weak in those systems so that we can implement what needs to be implemented at the local level.

Senator ROSEN. That is a great suggestion, because we need to get it out to every school district, large and small.

Another thing that we may have to do in order to do this, is our cybersecurity surge capacity. Ms. Huey, in your testimony you note that Ohio has created a civilian Cyber Reserve, consisting of a volunteer force of trained cybersecurity civilians to assist in a variety of cybersecurity needs. Senator Blackburn and I recently introduced the Civilian Cyber Security Reserve Act to establish a civilian Cyber Reserve at DHS and the Department of Defense (DOD) to call up cybersecurity experts at our times of greatest need.

Ms. Huey, how has the Ohio Cyber Reserve helped reduce cyber threats to the State, and what are some lessons you think that we could draw on what you have done and apply that to the national level in order to supplement DHS's existing personnel and add additional cyber capacity?

Ms. HUEY. Thank you, Senator, for that question. The Ohio Cyber Reserve operates much in the way that you were pointing out. It was introduced by OC3 and then it was authorized by the Ohio General Assembly in 2019, and it really does operate like a military reserve. It is under the adjutant general. It can be activated by the Governor.

Currently we are in the process of building out ten regional teams across Ohio. We have three of those teams already stood up and running. They do not publicize when they are deployed, but they have been deployed, and they have been successful.

I think there would be a lot of lessons learned and information that we could share with the new program at the Federal level as to how we identified that expertise, because we really wanted a cross-section of expertise, people that know the latest but also people that know how to deal with legacy systems as well. Thank you.

Senator ROSEN. I think I am going to have my team reach out to you and see what some of the lessons learned and best practices are, and we can see what we can do with those here.

I think when we talk about this, what I would like to ask, especially to the mayor, as you are dealing particularly at the local level, when we are talking about all the cybersecurity personnel and implementation and setting standards, and we do have to do all of that. But we really have to create a trained workforce, not in cyber but really a technologically savvy workforce, because there is not an area that someone is not going to have to be aware of a phishing scheme, any way that the vulnerabilities and multiple ways that people get in.

Mayor Schewel, can you describe the resource and workforce constraints that you may have and perhaps how we might consider a career in technical education down at, I guess, the city level or school districts, and they could be city or county, to try to really increase workforce talent and capacity, because at the end of the day, they are the faces on the other side of the computer that may be the ones that get taken advantage of unknowingly, and that hurts all of us.

Mr. SCHEWEL. Senator, thank you very much for the question. You are absolutely right. I think there are two aspects to that. One is—and Judge Whitley spoke to this early—the ability to train our young folks within the city to avoid phishing attempts, which is the way this successful cyberattack happened against our city. We were fortunately backed up, but that is the way people got in. I think that kind of training is critically important, and we do a lot of that. It cannot only be training, though. Multi-factor authentication, those kinds of things, are also critical.

But I also think that there is the issue of having the—we live in the Research Triangle region of North Carolina. We have highly trained technical workforce, and making sure that we have enough of those people on staff is really important. That is one of the reasons I think it is really important that we have additional funding. It costs us $900,000 a year to do our IT security. It is very expensive, and we need support for it.

Senator ROSEN. I guess I have a few second left, but what I would like to say is I think—and it is not a question of this Committee, but I do think that we have to increase our STEM edu-

cation across the board, I would say pre-K through 12, so that they are ready to work right away, in all these areas, to protect whatever business, government, whatever they go to do as an adult. I look forward to working on some of those things in the future.

Thank you, Madam Chair.

Senator HASSAN. Thank you very much, Senator Rosen.

I have additional questions, and I am going to check with the staff. That is all the Senators we have lined up right now, right?

I thank the panel for so much excellent testimony, and I do have a few more questions. I am going to start with a question to Ms. Huey.

Collaboration among States could serve a really important role in bolstering cybersecurity, and you have referenced that a bit already this morning. Ms. Huey, do you think multi-state cybersecurity projects would boost cooperation among States and improve cybersecurity beyond what States could achieve alone?

Ms. HUEY. Thank you for that question, Senator. I absolutely do, and I do not believe that there has probably been enough done at that level. Ohio Homeland Security is currently in the process of surveying all of the State's fusion centers, just to get a real good feel on what their cyber structure looks like. We want to benchmark ourselves and see if we are doing well. In the conversations with our surrounding States, there is a lot of interest and a lot of communication, and I think there is some ability to really work on some collaborative projects.

Additionally, I think the Federal Department of Homeland Security has a number of centers of excellence, partnered with universities, and I think that would be a real opportunity as well, that should be explored.

Senator HASSAN. Thank you for that.

Mr. Lips, I want to turn to you, obviously, it is something you have talked about in your testimony and in the purview of this Subcommittee, we have a duty to ensure that taxpayer dollars are spent efficiently and effectively. In this case, the goal is to efficiently and effectively spend grant funds to reduce the cybersecurity risk of State and local entities.

How do you think the Federal Government should measure how effective grants are at reducing State and local cybersecurity risk, and how should this be integrated into the grant program?

Mr. LIPS. Senator, thank you for the question. I think that is a great issue to be raising, particularly if Congress is considering establishing a new, dedicated cybersecurity grant program. It is one of the lessons, I think, that we have learned over the past 20 years with the FEMA grant program. That program was originally intended to be risk-based and focused on helping States and urban areas buildup capabilities that were needed, particularly after 9/11.

Unfortunately, over time, my view is that that program has become more of a formula-based program that is no longer essentially risk-based, and as GAO and others have pointed out, FEMA has struggled to measure how States are buying down risk.

Senator HASSAN. Right.

Mr. LIPS. With a cyber grant program, I would urge the Committee to be focused on—starting from the beginning, of ways to

measure that, to not be looking back years later and think, this should have been more risk based.

Senator HASSAN. OK. Thank you. I want to turn back to the issue that Senator Ossoff was talking a little bit about, which is information sharing. To Mayor Schewel, to Judge Whitley, and to Mr. Lips, information sharing has been one of the key ways that the Federal Government supports State and local cybersecurity. However, there are many questions about how the information sharing regime could be improved.

Mayor Schewel and Judge Whitley, how useful has the information that the Federal Government shares with you been, and are there other types of information that the Federal Government could provide that you would find useful? I will start with you, Mayor Schewel, and then go to Judge Whitley.

Mr. SCHEWEL. I will tell you, Senator, I do not honestly know the answer to that question in detail. I can tell you that we have really needed our Federal Government partners, including the FBI at times, during our recent cyberattack. But I am sorry, I have to get back to you on real information about the usefulness.

Senator HASSAN. Sure. OK. Thank you. Judge Whitley.

Judge WHITLEY. I know that our IT folks are in constant communication not only with the Federal agencies, also with the local. They are meeting on a monthly basis or a quarterly basis. Then any time any particular event happens, then they are working with one another and helping one another out. Any type of collaboration that can occur needs to be encouraged, because that is the way that we will keep people up to date on what the new style or the hack of the day is, and go under that type of a scenario. But the Feds have been very helpful. I know our folks are members of just about any organization they can become a member of that will assist or will help in identifying threats or things that are going on in the community.

Senator HASSAN. Thank you. Mr. Lips, how do you think we can improve cybersecurity information sharing between Federal, State, local, and Tribal organizations?

Mr. LIPS. Thank you for the question, Senator. Generally I think that information sharing programs have been very well intended and have been a step forward from where we were a decade ago.

That said, the various watchdogs, like the inspector general, have identified challenges within DHS's information sharing programs, issues such as timeliness, over-classification, and frankly, general value of the information that is shared has resulted in limited participation from the private sector, from what I understand, and from what the IG has found. I think addressing these areas and open recommendations broadly, both for private sector partners as well as State and local governments would be a valuable improvement.

In addition, I think there is valuable information sharing that can be provided about security recommendations, from supply chain acquisitions risks, also just general best practices having recommendations be made in a way that is prioritized would be really helpful for organizations across the board, including State and local governments.

Senator HASSAN. Thank you. I want to ask a question of all the government witnesses now about Homeland Security Grants, because there has been a little bit of discussion about what already exists, and I want to really try to drill down on the effectiveness and usefulness of that.

The Department of Homeland Security provides grants that can be used for a variety of purposes, including, as has been pointed out, cybersecurity. The State Homeland Security Grant program used to require that recipients use at least 5 percent of these grant funds for cybersecurity, but that has now been increased to 7.5 percent. That was done earlier this year. It also requires that a portion of these funds pass through to localities.

My question to all our government witnesses is whether these requirements are enough to address cyber needs? Judge Whitley, Mayor Schewel, and Superintendent Holden, have any of the local entities you represent received funding through the State Homeland Security Grants for increasing your cybersecurity? I will start with Judge Whitley.

Judge WHITLEY. We have received funding but this is one of the things that because of the increase in activity we do need more funds. I know that that is the standard answer you feel like you get any time you ask a governmental entity about any particular issue, but I think we all recognize, just as we stated earlier, about the very public threats and confidential, where they come in and seize operations or stop operations from happening. This is an ever-increasing area of threat, and we need to be focusing more and more dollars and efforts on that.

Senator HASSAN. Thank you. Mayor Schewel.

Mr. SCHEWEL. Thank you, Senator. I think it is really important that we not be cannibalizing other Homeland Security programs to do this cybersecurity work. We are going to need all of it. The cybersecurity threats that we are facing, every day there are cybersecurity attacks on the city of Durham, and we are able to fend them off. But all the actors have to do is be successful once. Our needs in this area are going to be greater and greater. We are going to need funding that is not competitive and not cannibalizing other Homeland Security funding. I think that is really going to be critical to us.

Senator HASSAN. Thank you. Superintendent Holden.

Mr. HOLDEN. I am unaware of any funding that we have received at the local level regarding the Homeland Security Grants. I have to look, though, past funding. I think really what I am looking for is more information. I think the more information that can be given to me at the local level from Homeland Security or from the State would be much more beneficial for me to be able to implement systems that will help us from these type of attacks.

Senator HASSAN. Thank you. Ms. Huey, in your view is the increase from 5 percent to 7.5 percent enough to improve State and local cybersecurity, or is there more assistance needed?

Ms. HUEY. Thank you for your question, Senator. I believe that there is more funding needed. I do not believe just increasing from 5 to 7.5 percent really recognizes the need for cybersecurity funding and the importance of the risks across our States. In fact, with

Ohio, our total Homeland Security award went down, even though the carve-out for cybersecurity went up.

I just think we keep making the pie smaller and then putting another priority in that, really does not do justice to what we need for cybersecurity across the country.

Senator HASSAN. Do you think a dedicated grant program would better ensure that State and local cybersecurity needs are met?

Ms. HUEY. I do. I do believe it will, because I believe that we could do more planning, more coordination, and really work better with the local governments and the small business to bring everybody up to a level that we want them to be.

Senator HASSAN. Thank you.

I have a couple of more questions if the witnesses will indulge me. I thank you. The testimony has been terrific, and I want to get to a couple of more things and make sure that there are not any other Senators who want to pop in and ask questions.

Let me go to this one now, to Superintendent Holden, Mayor Schewel, and Judge Whitley. It has become increasingly clear how important cybersecurity is for all organizations. However, some officials in charge of setting priorities may not fully appreciate the vulnerabilities of their cyber systems. You all clearly pay more attention to cybersecurity issues than many others may.

Superintendent Holden, Mayor Schewel, and Judge Whitley, do you believe that creating a State and local grant program dedicated to cybersecurity would encourage officials to focus more on it, and how might that increased engagement boost cybersecurity beyond just the extra resources that a grant program would provide? We will start with you, Superintendent Holden.

Mr. HOLDEN. Thanks for the question. Yes, I think a grant program and a committee to look at these things at the State level would absolutely highlight the need and the ability to continue to focus on these things. New Hampshire votes all State, whether it is through the Superintendents Association, through the Department of Education. I think the more attention that could be given in this small State, where we have a very locally committed but yet regionally organized, I think would absolutely benefit our ability to address some of these issues.

Senator HASSAN. Thank you. Mayor Schewel.

Mr. SCHEWEL. Thank you very much, Senator. Yes, definitely, we really need such a program, again, when I think about our small cities and how this would not just help them with funding but help them with the kind of coordination that you talked about. Again, 80 percent of cities in this country are below 50,000 people in population, and their ability to do the work that they need to do for cybersecurity, they just simply cannot do it on their own.

A grant program that would encourage the kind of cooperation necessary would be an incredible boon to those small cities. It would be good for all of us, but I think especially for our small municipalities it would be essential.

Senator HASSAN. Thank you. Judge Whitley.

Judge WHITLEY. I think anything that helps in the coordination and the collaboration of understanding the issues and the problems will be very helpful. All too often, anyone who is affected is very reluctant to get out there and announce that they have been af-

fected. Sometimes you feel like, OK, we are small enough, we will slip under the radar, and in today's environment that is just not happening.

I think the more you can bring folks together, whether it be on a statewide basis or a regional basis or a county-wide basis, to talk about what is going on and to make people aware of some of the issues, that is going to be beneficial. That is going to maybe result in them allocating a few dollars that they have not allocated before, to help address, or to be prepared and understand that maybe your backup system was broke a week ago, and had you not done that, look at the effect that it would have had once you did get hit.

The more collaboration that we can have with all of the entities around us, the better off we will be.

Senator HASSAN. Thank you. Ms. Huey, would you like to provide your perspective on this?

Ms. HUEY. I would agree with what the other witnesses were talking about. I think this is not an urban issue. When we think about criminal justice funding or some of those things we focus on big-city problems. This is a problem all across our local governments, regardless of size. Having the ability to help out the ones, as the mayor pointed out, with the smaller budgets, I think is critical. Again, that standard of preventive preparedness that we can bring everybody up to.

Senator HASSAN. Yes, I sometimes think people forget that coordination and preparedness takes resources. You can be well intentioned in it but if you do not have people who can spend the time doing it, it gets difficult to actually accomplish.

Because I have the time, and I know, Ms. Huey, you have mentioned this too, I want to ask one more question to you, and then in a wrap-up question to all of you. I am going to preview the question so you can think about your answer. When we close I would like you to think about one piece of advice each of you would give to your colleagues working in State, county, local, or Tribal government when it comes to cybersecurity. That will be the final question.

But first, Ms. Huey, I want to talk to you a little bit about the National Guard's role here. Earlier this year, Senator Cornyn and I reintroduced the bipartisan National Guard Cybersecurity Support Act. This legislation explicitly authorizes the National Guard to provide cybersecurity support services at the request of a State Governor, to be performed as training duty upon approval by the relevant service Secretary.

Ms. Huey, can you speak to the role that the National Guard plays in Ohio's cybersecurity, particularly as a part of the larger plan for how Ohio is improving the cybersecurity of State and local systems?

Ms. HUEY. Absolutely. Thank you for that question. As I indicated in my comments earlier, the Ohio National Guard really took a lead role in cybersecurity early on in Ohio. The Cyber Reserve was authorized by our General Assembly in 2019, and they really went out and recruited that civilian expertise that really existed already in the State, and they were very strategic about making sure that each regional team had the breadth of experience that could respond to a variety of attacks. That has been very successful, and

it is wonderful to see the Federal Government will be able to support that and backs that up. That has been something that we are very proud of here in Ohio.

The Ohio Cyber Reserve, the Cyber Range Institute, is also connected to that, and that is in some of our universities is really a think tank and a testing site, and it is very education focused. We have the existing expertise in the Cyber Reserve and the Cyber Range is trying to build that workforce development through our K–12 and our universities.

Senator HASSAN. Thank you very much.

Now the wrap-up question here, the one piece of advice each of you would give to your colleagues who are working State, county, local, or Tribal government when it comes to cybersecurity. Why don't we start with you, Mr. Lips, then we will go to Superintendent Holden, the mayor, and the judge, and then I will allow Ms. Huey to wrap it up.

Mr. LIPS. Thank you, Senator. One piece of advice I would offer to State, local, county, and other government officials working at that level is that it is very helpful for Members of Congress and congressional staff to hear your perspective about some of the challenges you are facing. In my testimony, I referenced the issue of compliance costs that the State CIOs have raised. It is very helpful to hear directly from State officials about what their day-to-day experience is and what those challenges are. I recall hearing from NASCIO and State CIOS in the anteroom several years ago, bringing that recommendation to my attention. There is great interest in their perspective, and it is very valuable to hear their view.

Senator HASSAN. Thank you, Mr. Lips. Superintendent Holden.

Mr. HOLDEN. Yes. I would let my fellow local and State folks know to be informed, to provide ongoing training and to implement needed systems, and that being proactive is a lot cheaper than being reactive.

Senator HASSAN. Thank you. Mr. Mayor.

Mr. SCHEWEL. Thank you, Senator. With your permission I will give two pieces of advice. One is to have an immutable backup of all data, including structured, unstructured, and binary data, and that is critical for quick recovery. We back up in Durham every 2 hours.

Then second, having an established partnership between Federal, State, and private sector parties so that if you are attacked, if you quickly define and contain the threat, we were able to do that and quickly set up a war room, and that is what really contained the cyberattack that we had. Thank you for that question.

Senator HASSAN. Thank you. Judge Whitley.

Judge WHITLEY. Again I want to thank everybody for the opportunity to speak today. The thing that I would say is test, train, perpetual, perpetual training and testing, to just keep at the front of everyone's minds that every time they are on that computer that there is someone trying to get in. The more we can do to keep our people thinking in that perspective, the better off we will be.

Senator HASSAN. Thank you, Judge. Ms. Huey.

Ms. HUEY. Thank you, Senator. My advice would be know your partners. Do not wait for the event to occur before you know who your resources are, your partners. Regularly communicate. There is

a saying in the EMA world, that a disaster is not the place to exchange business cards. You need to know who your network is, and your partners that are to help in a situation.

Senator HASSAN. Thank you so much. I want to thank all of the witnesses this morning for giving us so much of your time and sharing your expertise and your perspective and experience. It is really invaluable and it really does help inform the work of this subcommittee and the U.S. Senate. Thank you.

Your testimony here today is going to help us craft better bipartisan legislation to help State and local officials address cyber threats. The hearing record will remain open for 15 calendar days, until 5 p.m. on July 2nd, for submissions of statements and questions for the record.

The hearing is now adjourned.

[Whereupon, at 11:51 a.m., the Subcommittee was adjourned.]

APPENDIX

Opening Statement as Prepared for Delivery by Chair Maggie Hassan
Emerging Threats and Spending Oversight Subcommittee Hearing
"Addressing Emerging Cybersecurity Threats to State and Local Government"
June 17, 2021

Good morning. The Subcommittee on Emerging Threats and Spending Oversight convened today's hearing to discuss the threats to state and local entities from cyberattacks and the consequences of those attacks on national security, the economy, and the lives of our citizens. We will discuss what state and local entities need to be able to effectively respond to cyber threats, and how the federal government can best support state and local authorities as they work to combat the growing wave of cyberattacks.

While the SolarWinds, Colonial Pipeline, and JBS meatpacking cyberattacks rightly received a lot of attention in recent months, state, local, and tribal entities have also faced serious cyberattacks that can cripple services for citizens and decimate local budgets. The cybersecurity firm Emsisoft estimated that the total cost of publicly known ransomware attacks on state and local governments in 2020, including costs to restore functionality and services, was nearly one billion dollars. A report from cybersecurity firm Blue Voyant found that there was a 50 percent increase in the number of cyberattacks against state and local entities from 2017 to 2019. At the same time, the average ransom demanded in those attacks increased 10 times, and the average cost to taxpayers to clean up after a single cyberattack rose to the millions of dollars.

Today's hearing sheds a light on the impact of attacks like the one we saw on Sunapee School District in my home state of New Hampshire, which is represented today by Superintendent Russ Holden. Luckily for the Sunapee community, the district had a plan in place, including a separate backup system, so it was able to resume operations soon after the attack was discovered, without paying the ransom. Thank you, Superintendent Holden, for your leadership on cybersecurity for school districts.

Amid the COVID-19 pandemic, we have seen more than ever the importance of shoring up cybersecurity. State and local agencies depend on digital delivery of services to Americans, and many state and local employees are also connecting to central networks from home in order to do their work remotely.

More investment, at all levels of government, is needed to strengthen cyber defenses. A 2020 survey of state Chief Information Security Officers found that most states only spend 1 to 3 percent of their overall IT budgets on cybersecurity, compared to about 16 percent for federal agencies. And many local governments, with their smaller budgets, are even worse off.

Cybersecurity risks will continue to rise if state and local entities aren't able to strengthen their cyber resilience. I am working across the aisle to help state and local officials address cyber threats, and increase information sharing at the federal, state, and local level.

I am pleased that the most recent National Defense Authorization Act included my provision to provide each state with a federally funded cybersecurity coordinator. These coordinators will

provide each state – and the local governments within them – with a local contact who can provide support and technical knowledge, and act as a bridge to the federal government. I was very happy to recently learn that New Hampshire's coordinator came on board in the last week. In addition, this Congress, I introduced a bipartisan bill with Senator Cornyn to better enable the National Guard to support state and local government cybersecurity.

But we need to do more. That is why I am also working with my fellow Senators to craft a dedicated cybersecurity grant program for state and local governments.

I am excited to discuss these ideas and more with our five insightful witnesses today. Four of them represent a state, a county, a city, and a school district, and can help us better understand the unique environment that each have to operate within. They can also help us better understand which types of federal support may be the most effective. The fifth witness is an expert in federal cybersecurity policy and notably, a former senior staffer for the Homeland Security and Governmental Affairs Committee.

To all of our witnesses, I appreciate your willingness to testify, and I want to thank you all for the role you play in helping to keep us safe. I look forward to learning from you today.

Senator Rand Paul
Opening Statement
Hearing of the Subcommittee on Emerging Threats and Spending Oversight
Senate Committee on Homeland Security & Governmental Affairs
"Addressing Emerging Cybersecurity Threats to State and Local Government"
June 17, 2021

Thank you Chairwoman Hassan, and thank you to our panelists today for your time. I look forward to hearing from each of you.

I'd like to begin my remarks with an observation, which is that the recent wave of ransomware attacks seems to have broken through into the public consciousness.

I traveled my home state of Kentucky extensively during the state work period earlier this month and was asked more questions about cybersecurity in those 10 days or so than in the previous 10 years.

Of course, we as policymakers have been concerned about malicious activity in cyberspace for some time now. In fact, at the Chairwoman's request, this subcommittee held a hearing on ransomware and cybersecurity this past December, and I'm grateful for her continued focus on this issue.

But from what I saw and heard from the people I represent, there's now a much more widespread appreciation for how disruptive these attacks can potentially be.

Obviously the Colonial Pipeline interruption and the specter of gas shortages was a major concern.

The Kentuckians I spoke to were also *very* concerned about the ransomware attack affecting North American meatpacking facilities owned by JBS, which may not have received quite as many headlines as the Colonial Pipeline incident, but which is every bit as alarming.

Clearly we have a problem on our hands. The nation must be able to secure its food supply and deliver fuel where it is needed. Recent cyberattacks have also targeted hospitals, school systems, water systems, and other essential services.

So how do we combat this?

As the old saying goes, an ounce of prevention is worth a pound of cure. Cybersecurity must be prioritized in the same way that any other essential services are prioritized.

As we will hear, recovering from cyber incidents such as ransomware attacks, and data breaches is several orders of magnitude more costly than what it takes to implement and maintain good cybersecurity practices on the front end.

Finally, I believe Congress needs to make sure that the federal government's role in detecting and responding to cyberattacks is limited and clearly defined, and that federal cybersecurity personnel are focused first and foremost on the security of federal information networks.

Senator Rand Paul
Opening Statement
Hearing of the Subcommittee on Emerging Threats and Spending Oversight
Senate Committee on Homeland Security & Governmental Affairs
"Addressing Emerging Cybersecurity Threats to State and Local Government"
June 17, 2021

The government can and should share information on threats and best practices with the private sector and state, local, tribal and territorial authorities.

However, Congress must keep critical infrastructure operators and state, local, tribal and territorial governments in the proverbial "driver's seat" on cybersecurity.

I am particularly worried about a proposal that recently passed the House of Representatives, which would create a new multi-billion dollar grant program to subsidize state and local cybersecurity.

The Washington solution seems to be to throw money at every problem, with the result being a $28 trillion national debt.

As Americans, we face cybersecurity concerns that involve the availability of gasoline, and the food supply, and the electrical grid, water and sanitation systems, and our communications networks – indeed, some of the fundamental building blocks of our society.

I look forward to the conversation, and again, to the witnesses, thank you for your time.

Statement of

Karen Huey

Homeland Security Advisor for the State of Ohio

Assistant Director, Ohio Department of Public Safety

United States Senate
Committee on Homeland Security and Governmental Affairs
Subcommittee on Emerging Threats and Spending Oversight

"Addressing Emerging Cybersecurity Threats to State and Local Government"

June 17, 2021

Introduction
Chair Hassan, Ranking Member Paul and members of the Subcommittee on Emerging Threats and Spending Oversight. My name is Karen Huey, and I am the Assistant Director of the Ohio Department of Public Safety. I also serve as Homeland Security Advisor to Governor Mike DeWine and am a member of the Executive Committee of the Governors Homeland Security Advisors Council. We appreciate the opportunity to share Ohio specific concerns and information with you this morning.

The topic of today's hearing is of great concern to many, and although I speak with you today from the state of Ohio, I know many of my colleagues across the country would echo these same concerns.

Our goals are to enhance cybersecurity across the United States and educate Ohio's local governments and businesses on the importance of taking cyber precautions. Predictions of Cybercrime are estimated to exceed $6 trillion USD globally and could grow 15% per year. The Wall Street Journal June, 2021 interview of FBI Director Christopher Wray stated the FBI was investigating about 100 different types of ransomware and compared the current state of cyberattacks with the challenge posed by the Sept. 11, 2001 terrorist attacks. The damage created by cyber-attacks are well known. Today I would like to share how we believe we could structure our limited resources to make the most impact in Ohio. Preventing cyber-attacks requires dedicated resources, coordinated strategies, and local commitment. Reports of cyber

intrusions and hacks are common, and the amount of time and resources necessary to recover from a cyber-attack is substantial. It can take months to rebuild systems to eventually make a local government, school system, utility, or business whole again. When successful, our state and local governments, critical infrastructure and businesses will have the tools to prevent future cyber-attacks.

Ohio is investing in and making strides in our efforts to strengthen cybersecurity. The Ohio National Guard has brought together more than 30 public, private, military and educational organizations to form the Ohio Cyber Collaboration Committee, known as OC3. The OC3's mission is to provide a collaborative environment to develop a stronger cybersecurity infrastructure and workforce. OC3 has established four subcommittees to help it achieve its primary goals: the Charter & Governance Public Awareness subcommittee, the Education/Workforce Development subcommittee, the Cyber Range subcommittee, and the Cyber Protection and Preparedness subcommittee. These committees are composed of Ohioans with a wide range of cyber and educational expertise dedicated to making Ohio a leader in how to integrate public-private partnerships into solving the cybersecurity problem.

While I have time to share only highlights, I definitely want to mention OC3's great progress with its Cyber Range Institute, which is a virtual training ground and testing site designed to enhance cybersecurity in Ohio. The Range was developed for and used by the Ohio National Guard, schools: from K through 12 and Universities, governments and businesses to train our cybersecurity workforce, to conduct research, test emerging technologies and host cybersecurity exercises and competitions.

Ohio designed a mechanism to bring existing cyber talent to the fight by authorizing the Ohio Cyber Reserve. Formulated by the OC3's Cyber Protection and Preparedness Subcommittee and authorized by the Ohio general assembly in 2019, the Ohio Cyber Reserve consists of a volunteer force of trained cybersecurity civilians, with the goal to function as a military reserve. They are organized in regional teams under the command of the adjutant general. The Cyber Reserve may be called up by the governor to assist government, critical infrastructure, businesses and citizens in a variety of cyber needs. Regional teams are being created and trained, with future duties to include assessing entities for cybersecurity vulnerabilities and making recommendations aimed at reducing cyber threats.

OC3's education and Workforce Development Subcommittee has done substantial work. It was responsible for identifying critically needed skills and it developed training and educational paths to provide skilled workers in the field of cybersecurity. This subcommittee was responsible for encouraging further development of cybersecurity in both K-12 and higher education. Finally this subcommittee trains users at all levels in good cyber hygiene and best cyber practices.

What constraints are we and local governments facing? As this subcommittee is aware, states have been receiving Homeland Security grant funding since 9-11. It has allowed us to build fusion centers, harden targets, identify critical infrastructure and form relationships across sectors that never worked together before. A great example of this occurred last week in Ohio and highlights one serous situation where the federal government's support to the states, locals and territories was felt.

Ohio's dedicated federal homeland security intelligence officer shared information about two Chinese video surveillance technology companies whose products have been banned for purchase or use by federal government agencies since 2018. Despite the federal ban, dozens of these systems were purchased in Ohio, including some school districts, and at least one hospital. In turn, Ohio Homeland Security (OHS) drafted a situational awareness bulletin designed to alert Ohio entities that these companies are likely using their products to provide U.S. customer data to the Chinese government for espionage and surveillance operations. OHS shared the bulletin using the relationships built with homeland security grant funding, including OHS' contact and information system, and forwarded to all Ohio Intelligence Liaisons and Ohio Public Private Partnership members. Almost immediately, responsive emails and phone calls from concerned representatives from Ohio entities that had purchased these products were being received and addressed. High level technical mitigation information has already been shared and CISA personnel are working on a plan with the affected entities that will include a more detailed risk management solution.

Ohio uses homeland security funding to support traditional capabilities, such as interoperable communications, search and rescue capabilities, hazmat, and information and intelligence sharing. Local entities used homeland security funding to build out capabilities to prepare for and respond to critical incidents to sustain a level of preparedness. Current funding is also used to support three fusion centers across the state of Ohio. In addition, we use these funds to support local projects across the eight homeland security regions. With the inclusion of cyber as a priority, Ohio's local governments are struggling even more to address the traditional preparedness needs while also prioritizing cyber projects. As homeland security funding has been static or reduced in the past cycles, forcing cyber into the homeland security grant process reduces already limited funding even further.

As the seventh largest state, with a population over 11 million, Ohio currently receives $6.7 million in homeland security funding. The current carve out for cybersecurity is less than $340,000.

I would assert that continued use of a small portion of homeland security grant dollars both takes away from the needs of traditional homeland security efforts and minimizes the importance of cybersecurity and its impact on state and local governments.

We would urge Congress to consider a dedicated grant program that will enhance Ohio's ability to focus on cybersecurity capabilities. Ohio's annual Stakeholder Preparedness Review identifies gaps in cybersecurity including planning staffing, equipment, training and exercising. Due to sporadic and uneven funding, Ohio's local governments find it challenging to formulate plans that address many of those gaps. Cyber-attacks are not limited to our major cities, and developing strong prevention, education and tabletop exercises will take time and resources.

In light of the resource constraints already mentioned and the increasing volume of cyber incidents, a dedicated program will help ensure we remain prepared for traditional terrorist events and cyber threats, without having to choose between them. It allows state and local Homeland Security efforts to remain focused on terrorism and safety while allocating additional funds to cyber to ensure both state and locals are prepared to respond and mitigate the damages from a cyber-attack.

Dedicated grant funding can be used to develop more robust cyber capabilities at the state level to provide guidance and assistance to local entities that lack the funding and infrastructure to implement cyber programs on their own, or who look to the state for leadership, guidance, and standards.

Three main areas identified for dedicated funding:

1. The state would share industry developed standards with its local governments, critical infrastructure and small businesses. The state would also offer assessments of current systems to improve where gaps are identified and direct local governments to resources. This is especially important for smaller local governments and businesses that do not have resources. In addition, the state would use existing homeland security procedures to ensure that any funding source created would receive monitoring to ensure compliance with grant requirements and appropriate infrastructure to manage grant funding.
2. The state would provide education and training to local governments, critical infrastructure and business entities that will include cyber exercises, end-user training, resources and guidance documents.
3. The state would make improvements to existing secure communication platforms that will be used to gather and disseminate important timely cyber information regarding threats to trusted partners.

Additionally, Ohio recommends that if cyber is a separate funding source, that federal guidance require as a condition of funding that local governments and businesses share indicators of compromise with the state to include: offender IP addresses, offender email addresses, the source of infection, if known, occurrence timelines and investigator contact information. Understanding the scope of the problem will identify better strategies, prevention and mitigation plans. If adopted, we also strongly recommend federal protection of the entity's information related to the existence and details of the cyber incident. Governments and businesses alike will be reluctant to share news or details of cyber incidents when the information could be shared publicly.

Ohio recommends that a dedicated funding source for cybersecurity be set aside or granted in addition to existing homeland security grant funds to build and sustain cybersecurity programs and projects over multiple grant years. This will allow Ohio to develop longer term strategies in partnership with our CISA Cybersecurity Advisor and other federal, state and local partners, ensuring the dollars allocated are a wise investment and produce measurable results.

In closing, many states, just like Ohio, recognize the importance of responding to cyber incidents and building a level of preparedness with our local governments. Our hope is that a dedicated cyber grant program can be created to help state and local governments thoroughly develop robust cyber capabilities to be able to combat the sophisticated efforts of cyber criminals. With many demands on budgets it is difficult to divert such resources or make an impact with only small amounts of funding scattered across the state. We also highly encourage adding a requirement of after action reporting so we can all learn from and be better prepared for incidents in the future.

We appreciate this subcommittee's commitment to addressing cybersecurity threats to state and local governments and hope to continue working with you to implement some of the strategies recommended in the testimony presented today. On behalf of the State of Ohio, thank you for the invitation to testify.

Written Statement for the Record

The Honorable B. Glen Whitley

County Judge, Tarrant County, Texas

On Behalf of the National Association of Counties

for the hearing

"Addressing Emerging Cybersecurity Threats to State and Local Government"

Welcome and Introduction

Chairwoman Hassan, Ranking Member Paul, and Members of the Subcommittee, my name is Glen Whitley and I serve as County Judge for Tarrant County, Texas. I also serve on the Board of Directors as Past President for the National Association of Counties (NACo). It is an honor to participate in today's hearing on behalf of Tarrant County, NACo and our local intergovernmental partners across the country.

As the 15th most populous county in the United States, Tarrant County is a hard cyber target. Our county is probed, scanned, phished, and outright attacked roughly 950 times per hour on a good day. While each county is unique, all county governments share core challenges to serving as stewards of public property, safety, and welfare. My remarks today will not only highlight the specific cyber priorities for Tarrant County, but also the overall challenges facing counties of all sizes.

The New Theater of War

In just the past year, we have seen several cyber exploitations that caused major disruptions across the United States. These attacks – including the Microsoft Exchange exploit, SolarWind's spyware breach, the Colonial Pipeline shutdown, and the JBS meat processing hack – all demonstrate exactly how vulnerable our nation's cyber security infrastructure truly is.

At the local level, we have experienced multiple ransomware attacks in recent years. Pinellas County, Florida, for example, recently experienced an attack on their water treatment facility allowing hackers to boost the level of sodium hydroxide in their water supply. As county reliance on technology increases, these attacks will likely increase as well.

Not only are these attacks endangering national security and costing billions in ransom and repair costs, but they also have a direct and lasting impact on the wallets of our residents. Unfortunately, cyber security experts expect these threats to escalate and possibly correlate with critical government activities like elections and tax collection. Online attacks to domestic

cyber infrastructure are quickly becoming the battlefield of choice for bad actors in the 21st Century.

Restrictions on Resources

To better understand how local governments are able to respond to cyber threats, it is important to start with the underlying challenges to local revenue and resources.

General revenues from local property taxes are the backbone of county funding because they are not restricted to a particular activity. Unfortunately, outmigration in many rural counties is reducing the local tax base while 43 states are imposing some type of limitation on counties' ability to increase local taxes.

Restrictions on federal and state resources also remain a challenge. Locally collected general revenues are not restricted to a particular activity and offer counties the flexibility needed to provide mandated services while addressing the unique needs of their communities. Unfortunately, about 93 percent of the state and federal funding used by county governments is restricted to a specific function. [1]

Matching requirements for federal grant and loan programs also make leveraging federal resources impossible for many counties. Subsequently, counties are increasingly forced to fund mandated services with general revenues and charges.

In recognition of lost revenue due to the COVID-19 pandemic, the American Rescue Plan (ARP) Act included $61.5 billion to county governments. Counties thank Congress for making this historic investment in America's counties. However, the U.S. Treasury prevented local governments from using these ARP dollars as a non-federal match for grant and loan programs. As counties now look for ways to leverage this critical assistance – many federal grant and loan

[1] https://www.naco.org/articles/counties-still-challenged-recession%E2%80%99s-recovery

programs will remain out of reach. Without relieving the pressure on county needs elsewhere, counties will struggle to invest in the cyber security infrastructure they need.

County Roles and Core Cyber Priorities

Counties are responsible for delivering a broad array of programs and services that provide a foundation for strong and stable economies. Collectively, counties own or operate thousands of hospitals, public health departments, water and waste management centers, jails, and emergency operations centers – all of which create significant cyber vulnerabilities. Without robust and reliable funding, these local assets expose our communities and these critical programs and services.

To help centralize assistance and best-practices, NACo's Tech Xchange provides county IT leaders an opportunity to diagnose and dialogue over cyber-related challenges. Additionally, a recent NACo survey found that 40% of counties placed cybersecurity as their #1 challenge for county IT.

It is important to note that cyber security needs are not only driven by exposures and vulnerabilities, but also by counties looking to meet certain national standards such as National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS) controls.

In Tarrant County, we adhere to the core principles of the NIST Cybersecurity Framework (NIST CSF) which are Protect, Detect, Respond & Recover. Achieving and maintaining these core principles requires an Information Security Program (ISP) that includes policies, procedures, and resources. While policies and procedures can be downloaded and customized, resources require continuous funding.

More generally speaking, county cyber resources are typically directed to three main areas – Education and Access, Infrastructure, and Preparedness.

Education and Access

It is regularly stated that an organization's greatest cyber weakness is the end user or employee. This is no different for local governments. A recent Cybersecurity Survey conducted by TalentLMS on behalf of Kenna Security found that 70% of employees polled said they recently received cybersecurity training from their employers, yet 61% failed their basic quiz on the topic.[2] In terms of access, it is a well-known best practice to only grant the level of access that is needed for one to fulfill their responsibilities. Yet, we often hear of cyberattacks that resulted in the bad actor gaining access to the county network because an end user had a higher level of access than they needed. A county of Tarrant County's size would expect to send roughly $50,000 on education and security awareness testing campaigns each year alone.

Infrastructure

One of the most basic best practices in the current environment, is the implementation of multi-factor authentication. Similar many online banking operations, this multi-factor approach is vitally needed in local government. Yet, it is a challenge for many counties to implement, from both an IT resource and cost perspective. Other infrastructure needs include updating and replacing network devices to stay ahead of evolving threats. Further, being able to vet cloud software and infrastructure providers as well as the supply chain requires time, money, and skilled personnel. A typical urban county could expect to spend roughly $200,000 each year on detection and prevention systems.

Preparedness

Preparedness is the county's ability to effectively monitor the threats "knocking" at our doors. This requires either the implementation of costly tools or securing externally managed services to perform the task. Resources such as CISA and the MS-ISAC provide assistance for some of these measures. Finally, preparedness includes the development of security policies and incident procedures, as well as regular testing through cyberattack simulations or "tabletops." Counties need significant guidance, resources, and affordable solutions to implement these

[2] https://www.scmagazine.com/home/security-news/61-percent-of-employees-fail-basic-cybersecurity-quiz/

tools, as well as technical assistance for the development of sound standards. A county could reasonably spend around $100,000 annually on quarterly vulnerability and penetration testing.

In addition to these expenses, a county of Tarrant County's size should also expect to spend roughly $650,000 each year for the manpower needed to manage and maintain all of these operations.

Direct and Flexible Funding

The difficulty leveraging CARES Act dollars to address the COVID-19 pandemic exposed how important direct and flexible funding is for local governments. Congress improved on these challenges through the American Rescue Plan which provided direct resources to America's counties struggling to meet their budgetary needs. As you consider how to best allocate cyber security investments, it is imperative for federal resources to reach their intended targets as quickly as possible.

Understandably, block grants help to quickly move resources out of Washington. However, that does not always translate to efficient or effective dollars. We applaud Chairwoman Hassan's work ensuring that a robust investment in our nation's cyber security infrastructure recognizes the need for direct and flexible resources.

Local governments will carry some of the heaviest burdens to securing our nation's cyber infrastructure. Therefore, it is imperative for local governments to play a significant role in the development of state-wide cyber security plans. This requires a meaningful seat at the table – not just a ceremonial appointment for political allies.

To guarantee these resources reach their intended targets, block grants should also have strict pass-through requirements. Additionally, local governments should have the flexibility to adapt and apply those resources to fit the unique challenges of their communities.

Closing

In closing, counties need a strong federal partner that can provide direct and flexible resources that allow local governments to quickly adapt those resources to meet the unique needs of their communities. This is especially true for cybersecurity resources – local governments own and operate some of our nation's most critical infrastructure. Without dedicated federal resources, many of our counties will remain defenseless to cyber threats and the potential for irreparable harm.

STATEMENT OF

THE HONORABLE STEPHEN SCHEWEL
MAYOR, CITY OF DURHAM, NORTH CAROLINA
ON BEHALF OF
THE NATIONAL LEAGUE OF CITIES

BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

"ADDRESSING EMERGING CYBERSECURITY THREATS TO STATE AND LOCAL GOVERNMENT"

JUNE 17, 2021

Introduction

On behalf of the City of Durham and the National League of Cities, thank you for the opportunity to provide testimony to the Senate Homeland Security and Government Affairs Committee's Subcommittee on Emerging Threats and Spending Oversight on a critical threat facing our nation. We appreciate the attention that Congress is giving to ways in which federal, state, and local governments can better collaborate to protect our public networks, infrastructure, and critical services from disruption, destruction, and expense due to cyberattacks. Our nation's cities, towns and villages are deeply concerned about the increasing toll that ransomware and other criminal attacks are taking on our localities and are eager to partner with Congress to strengthen our cyber defenses and resiliency.

We appreciate the efforts by federal agencies such as the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Institute of Standards and Technology, as well as state leaders and National Guard detachments, for their partnership and assistance to help our cities, towns and villages prevent, survive, and recover from cyberattacks. However, we believe more can be done. Localities do not have enough resources, whether in capital or workforce, to adequately protect our networks across the nation. Our cyber adversaries are increasing the sophistication, frequency, and impact of their attacks more every year, while spending on cyber defenses has not kept up.

Most municipalities are underprepared for a cyberattack. It is not a matter of if, but when, most communities will face a serious attack. Additional resources for both state and local governments will go a long way toward empowering our communities to work together with states and federal agencies to plan, prepare, harden against, and be able to recover quickly from cyberattacks. However, to be most effective, new federal resources must encompass several key principles: they must provide dedicated new resources without cannibalizing existing grant programs and budgets; they must promote intergovernmental partnership and collaboration, and they must not impose one-size-fits-all mandates on the tens of thousands of local government units in the United States.

About the City of Durham, North Carolina

The City of Durham, known as Bull City, is a thriving city in the Research Triangle region of North Carolina, with 287,865 residents. Our city provides a variety of daily critical services to our residents, including operation of a water and stormwater system, transportation systems management and maintenance, police, fire and 9-1-1 answering services, and sanitation. We

employ 2650 employees in 24 departments. Despite benefiting from our size and proximity to a highly-qualified technical workforce, Durham has experienced its share of cyberattacks and this experience has led us to dedicate an increasing share of our technology services budget to cybersecurity.

On March 5, 2020, just as the full impact of the COVID-19 pandemic was beginning to be felt in the United States, both the City and County of Durham were hit by a ransomware attack. Throughout the process of halting, evaluating, and recovering our networks from the attack, the city's lights remained on. Public safety systems, including the 9-1-1 network, remained functional throughout, although the city did lose access to key networks while we went through the process of shutting down and restoring those files and systems from backup. The city was able to return to full levels of operation within only four days and took several weeks to reimage and harden our city's more than 2700 different endpoints, including 150 servers.

The City of Durham was fortunate to weather this experience with minimal disruption, but this was not an accident. Our city had planned in the months and years prior both to prevent such an attack, and to recover when an attack inevitably did occur. After a highly disruptive attack on the Durham Public Schools network in 2009 that impacted school operations for months, the City of Durham worked to put in place policies, procedures and plans to ensure that the City would not experience a similar costly disruption. The city established a comprehensive plan and budgeted for improvements over time. The city also established working relationships with the FBI, state leaders in North Carolina, and the Multi-State Information Sharing and Analysis Center (MS-ISAC). These plans were tested in 2018 when a second attack occurred, this time impacting the city's fleet vehicle network.

The lessons we learned from this process positioned the city to move quickly and decisively when attackers struck in 2020. The city was able to work quickly to form a war room with representatives from our staff, contractors, and other government partners, including the North Carolina National Guard, to respond to and recover from the attack. This was made particularly challenging as we navigated new social distancing protocols to keep our team safe and healthy throughout. However, because we had a plan and partnerships in place, including regular backups of all city data to the cloud, we were able to maintain functions critical for life and safety, and to restore full functionality quickly and without paying a ransom.

Local Governments are Experiencing an Unprecedented Quantity and Sophistication of Cyber Threats

Building strong cyber defenses for our nation's cities, towns and villages presents serious challenges. There are tens of thousands of local government units in the United States, ranging from very large cities like New York City and Los Angeles, to mid-sized and smaller cities like Durham, to the smallest rural towns. Municipal governments, regardless of size, often manage sensitive data about our residents and are responsible for systems critical to health and safety, including water and sewer systems, traffic control systems, public safety systems, sanitation, and more. The City of Durham operates a water utility. Other local governments may operate gas or electric utilities. As seen with the attack on the water system of Oldsmar, Florida this year, if bad actors are able to gain unfettered and undetected access to these critical systems, the consequences may not just be costly, but fatal.

Municipal systems are attractive targets for criminal actors. In recent years, local governments have become major victims of ransomware attacks, with at least $144.35 million in Bitcoin paid to criminals as ransom between the years of 2013 and 2019.[1] That figure does not include ransoms paid during the past year of increased attacks as organizations dramatically expanded virtual work environments, nor does it include the operational impact of downtime and recovery from ransomware attacks. The average downtime related to a ransomware attack is 9.6 days, and the recovery cost to impacted municipalities can easily reach the tens of millions of dollars.[2]

Over the past year, as many communities observed social distancing guidance, our cities were obliged to shift very rapidly to working and conducting public meetings remotely. This presented a very large new attack surface to criminal organizations. Suddenly, municipal employees were conducting the bulk of their work from potentially unsecured home networks, and local governments had to grapple with creating new ways to hold legally required public meetings that met standards of public disclosure and access, while also protecting the proceedings from things like Zoom-bombing. Our public information technology workforce has been in overdrive setting up our staff and elected officials with new equipment, training, and security awareness.

---

[1] Federal Bureau of Investigation, "The National Cyber Investigative Joint Task Force Releases Ransomware Fact Sheet," February 4, 2021. Available https://www.fbi.gov/news/pressrel/press-releases/the-national-cyber-investigative-joint-task-force-releases-ransomware-fact-sheet

[2] KnowBe4, "The Economic Impact of Cyber Attacks on Municipalities," 2020. Available https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf

Ultimately, a criminal organization only must be right once when attempting to breach our systems. Our local governments must be right every time. While communities like Durham have made great strides in recent years in terms of implementing the best practices outlined by organizations like NIST and increasing the level of awareness and cyber hygiene among our elected leaders and staff, these measures are not enough on their own. Cyber criminals rely not only on social engineering tactics and careless end users, but on sophisticated attack methods to penetrate and disrupt our networks. Protection in the future will require both increased training and awareness for our teams, as well as ongoing work to keep our systems updated, backed up, and continually monitored for threats and intruders. This will not be a one-time action, but an ongoing and continuously evolving process.

Cities, Towns and Villages Have Serious Capacity Limitations

Durham is fortunate to have a fantastic city staff team to guide our cybersecurity strategy and advise our council and city manager as we budget for cybersecurity and technology expenditures. Our city also has an active partnership with local academic institutions that is helping to build our local technology workforce pipeline and create opportunities for local students. For Fiscal Year 2020-2021, the City Council approved a General Fund budget of $214.6 million, of which $9.14 million supports our Department of Technology Solutions. This represents about 4.3 percent of our city's core budget. Our Technology Solutions program must support a number of other priorities and activities in addition to cybersecurity, including our city's general technical support for employees and systems across a wide variety of activities, our open data program, as well as our city's geographic information systems (GIS) activities in partnership with the County of Durham.

Information technology generally, and cybersecurity specifically, must compete with a wide range of other city priorities in all communities. The American Society of Civil Engineers estimates that the nation's infrastructure, much of which is owned and operated directly by local governments, requires $2.59 trillion more in repair and upgrades over the next decade than is currently funded.[3] This means that cybersecurity expenditures must compete directly with activities like filling potholes, repairing water systems, modernizing 9-1-1 answering centers, and maintaining parks, all of which are much more visible to residents.

[3] American Society of Civil Engineers, "Investment Gap 2020-2029." Available https://infrastructurereportcard.org/resources/investment-gap-2020-2029/

Cities are also under substantial budgetary pressure in terms of revenues. Cities, towns and villages in at least 48 states are limited by at least one state- or voter-imposed tax and expenditure limit, which can restrict the ability of localities to raise funds.[4] These can include limits on tax rate, tax growth or overall total revenue increases from common revenue sources like property taxes. Tax and expenditure limits can hinder the ability of municipalities to expand reserves and investments when the economy is performing well and limit the capacity for a community to respond in a crisis.

Small Municipalities Have Unique Challenges

The City of Durham is fortunate, but we have still needed to make tough choices. Other communities are much less fortunate. More than 80% of municipalities in the United States are small, with populations below 50,000 and substantially fewer resources than the City of Durham. In these smaller communities, staff and budgets are seriously limited, with a single information technology staff person responsible for a wide variety of functions, including security – if the community has a full-time IT staff person at all. In a 2020 survey of local government IT executives, the Public Technology Institute found that 65.2% of respondents felt that their cybersecurity budget was inadequate. Less than half of respondents indicated that their local governments had a cyber incident response and disaster recovery plan that was tested annually.[5]

Many local governments, including nearly all small local governments, outsource IT functions and services. It is difficult for most city governments to attract a stable, qualified workforce with the necessary qualifications to maintain a cybersecurity program, and frequently does not make business sense to manage all of these functions internally. However, it is not always clear whether vendors are upholding strict cybersecurity standards of their own, and outsourcing cybersecurity is not a foolproof strategy to eliminate risk. In 2019, 22 Texas cities and counties were impacted by a serious ransomware attack that gained access to the cities' networks via a common managed service provider.[6] Individual communities, particularly smaller communities, cannot ensure the

[4] National League of Cities, "Local Budget Pressures are Real. So Why Don't Cities Just Raise Taxes?" June 1, 2020. Available https://www.nlc.org/article/2020/06/01/local-budget-pressures-are-real-so-why-dont-cities-just-raise-taxes/

[5] Public Technology Institute/CompTIA, "2020 Public Technology Institute (PTI) State of City and County IT National Survey," October 29, 2020. Available https://comptia.informz.net/COMPTIA/data/images/2020/Misc/2020-PTI-State-of-City-and-County-IT-National-Survey.pdf

[6] ProPublica, "The New Target That Enables Ransomware Hackers to Paralyze Dozens of Towns and Businesses at Once," September 12, 2019. Available https://www.propublica.org/article/the-new-target-that-enables-ransomware-hackers-to-paralyze-dozens-of-towns-and-businesses-at-once

qualifications of all possible vendors, nor can they be responsible for managing the security of hardware and software supply chains upon which they rely.

In many ways, operating a smaller town or village poses similar challenges to those faced by small businesses. They have fewer resources, but are no less vulnerable to cyber threats, and the consequences for a cyberattack are no less serious in their communities than in larger ones. They are also just as responsible for the wellbeing and data protection of their employees and residents as a larger city is. Because of their smaller scale, it does not make sense to keep many cybersecurity or information technology services and capacities in-house. However, it is also difficult for these communities to stay on top of changing best practices, procure managed cybersecurity services, software as a service, and outsource technical staffing, because they have trouble achieving economies of scale and adequately vetting vendors.

Policy Solutions for Building a Stronger Intergovernmental Partnership

Local governments are under a serious and growing threat of catastrophic cyberattack. The risks to local health, safety, and economic stability cannot be denied. The federal government cannot solve this problem with mandates: requirements to implement stronger security measures, training, and technological solutions for response are out of reach for most municipalities without additional support. Even relatively simpler best practices, such as maintaining current hardware and software, applying patches and updates on recommended cycles, implementing cyber hygiene training across the entire user base, requiring multifactor authentication and password complexity for all users, and data backups, are substantial and ongoing expenses for local governments of all sizes. For larger local governments, these activities are important, if sometimes challenging, to prioritize and budget for. For smaller towns, they may be entirely out of reach.

The federal government has an opportunity to not just financially support these activities, but to partner actively with state and local governments to improve cyber resiliency across all levels of government. The National League of Cities recommends any new federal cybersecurity legislation address several core principles:

1. Provide sustainable new funding, without cannibalizing existing funds;
2. Actively promote planning, information sharing, and business partnerships between units of government; and
3. Avoid the temptation to apply a top-down, one-size-fits-all solution to widely varying sizes and forms of local governments.

Congress Should Provide Sustainable New Funding Without Cannibalizing Existing Funds

New sources of funding are desperately needed for local government cybersecurity – but they must not come at the expense of existing public safety or homeland security resources, and they must persist over time. While a one-time infusion of resources can help a city do one-time things, such as conduct needed network or hardware upgrades, conduct risk audits, or create an initial plan for risk mitigation and response, most cybersecurity expenses are ongoing. Network monitoring, staff resources to track and apply needed patches and updates, and data backups are all key elements of reducing cyber risk and recovering effectively from an attack, and they are all significant ongoing expenses that must be maintained and budgeted from year to year. A one-time grant can help kickstart additional activities around cybersecurity and make them more affordable, but a single grant will not be a silver bullet for cybersecurity.

These grants must be reasonably flexible to account for the kinds of expenses best suited to these single-use needs. For example, after taking over administration of the .gov domain following passage of the Consolidated Appropriations Act in December of 2020, CISA elected to fulfill its congressional directive to incentivize adoption of the .gov domain by making it available free to government entities.[7] This is an important step in removing barriers to transitioning to a more secure domain for local governments but does not account for additional costs related to domain transition, such as staff time to manage the process, redesign of municipal graphic materials, and reprints of signage, business cards, and other tangible resources. These additional costs may be significant enough to discourage a municipality from changing domains, and should be considered in new grant programs.

Additionally, new resources must not come at the expense of existing grants to state and local government from the Department of Homeland Security. The existing 7.5% carveout for cybersecurity introduced this year within the Urban Area Security Initiative and State Homeland Security Program grants ultimately serves to increase the number of things state and local governments are attempting to do with a finite budget, rather than sustainably increasing the support available for cybersecurity specifically. Congress should also consider not requiring, or minimizing, cost sharing for these programs to incentivize participation by eligible units of government.

[7] Dotgov, "A new day for .gov," April 27, 2021. Available https://home.dotgov.gov/2021/4/27/a-new-day-for-gov/

New Federal Cybersecurity Programs Should Promote Collaborative Planning, Information Sharing, and Business Partnerships Between Levels and Units of Government

Any new federal cybersecurity programs should prioritize promoting intergovernmental partnership and collaboration. While local governments are ultimately individually responsible for their own security, the federal government can serve as a key central distributor of information, resources and assistance, and state governments can play similar roles within their jurisdictions. For example, the North Carolina National Guard and local governments in the state increasingly collaborate on cyberattack prevention and response, and additional resources would support the enhancement of these efforts.

The Cyberspace Solarium Commission recognized the critical role of the federal government when recommending that the Cybersecurity and Infrastructure Security Agency be granted additional funding and authority to conduct larger-scale and more advanced assistance and coordination to partners outside the federal government.[8] As attacks on energy and water systems increase, clarity around federal agencies' respective roles in preparing for and recovering from cyberattacks is also critical to ensure that local governments are operating as effectively as possible in hardening their own cyber defenses and creating or practicing incident response plans.

Procurement of solutions and services is another area ripe for additional intergovernmental collaboration. As noted previously, cybersecurity challenges are particularly severe for mid-sized and smaller municipal governments. Regional government councils, states, and municipal leagues can play a key role in achieving economies of scale in procurement, distributing information, and providing support in response to cyberattacks. Larger entities should be incentivized to consider offering assistance in procurement, such as through state purchasing portals, access to statewide contracts, or provision of certain solutions or services at cost. Federal and state entities are also well-positioned to share information about qualified vendors and products that meet minimum performance or security standards, and the federal government is positioned to establish and uphold those standards for protocols, software, and hardware supply chains. By lowering cost barriers to these tools, as well as making it easier for local governments to ensure that the purchases and contracts they make individually are adequate, federal and state

[8] Report of the U.S. Cyberspace Solarium Commission, March 2020, p. 39. Available http://www.google.com/url?q=http%3A%2F%2Ffdd.org%2Fwp-content%2Fuploads%2F2020%2F03%2FCSC-Final-Report.pdf&sa=D&sntz=1&usg=AFQjCNEjLcRR29lrpmdRUZe1aFf2Bb6EGg

governments can make it easier for local governments to meet their responsibilities within the partnership.

Congress Should Not Apply One-Size-Fits-All Solutions to Local Governments

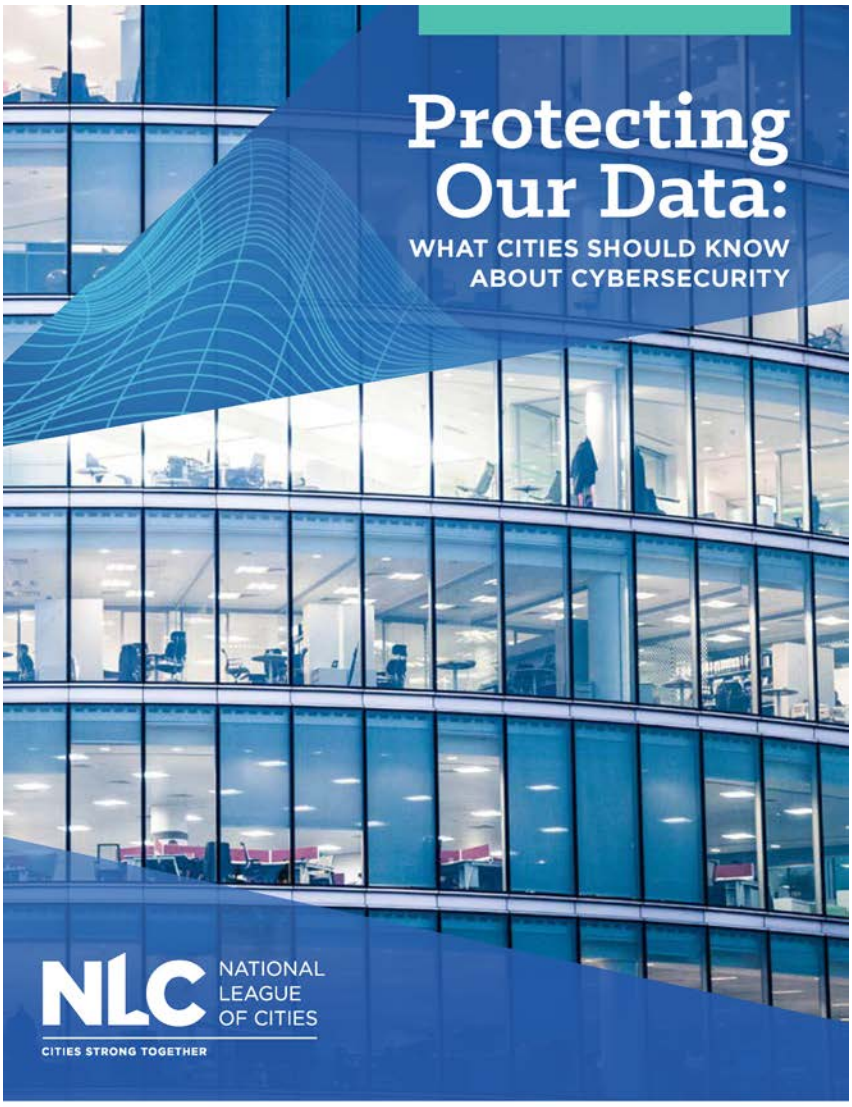
Lastly, Congress should avoid the temptation to apply a top-down, one-size-fits-all approach to local government cybersecurity. The largest cities have populations of millions, with tens of thousands of full-time employees, while the smallest towns and villages have populations measured in the tens and no full-time staff. Large municipalities are capable of effectively accessing and deploying direct federal grant dollars quickly, without additional processing through state entities, while smaller local governments may benefit from service provision or assistance through state entities. Each municipality has different assets, network architectures, and local resources available to them. Ideally, any new federal cybersecurity grant program should allow those municipalities capable of effectively managing a federal grant directly to do so, while also providing for state administration of dedicated streams of funding available to support smaller local governments.

Any state programs, whether cybersecurity incident response plans, grant systems, or business offerings, should be developed in collaboration with their local governments and with substantial local input. While federal and state agencies may bring to bear greater resources than most municipalities, they need the "eyes on the ground" provided by local officials, who have the most familiarity with their own systems, capabilities, and needs. Programs such as those outlined in the State and Local Cybersecurity Improvement Act rightly require local officials to have a seat at the table for all planning and advisory committees.

Conclusion

America's cities, towns and villages are eager to partner with the federal and state governments to harden our collective defenses against cyber criminals. Cyberattacks, whether ransomware or other forms of intrusion, are incredibly costly for local governments and represent serious threats to the life and wellbeing of our residents. However, we cannot adequately protect our nation's residents, economy, and infrastructure without substantial additional investment and partnership from Congress. The substantial, ongoing, and increasing expenses and actions necessary to secure our cities have outstripped the ability of many communities to keep up. The City of Durham and our fellow local leaders look forward to continuing this conversation with the members of the Senate as we develop a path forward.

APPENDIX


Protecting
Our Data:
WHAT CITIES SHOULD KNOW
ABOUT CYBERSECURITY
NLC
NATIONAL
LEAGUE
OF CITIES
CITIES STRONG TOGETHER

NLC NATIONAL LEAGUE OF CITIES
CITIES STRONG TOGETHER

pti Public Technology Institute
CompTIA

About the National League of Cities
The National League of Cities (NLC) is the nation's leading advocacy organization devoted to strengthening and promoting cities as centers of opportunity, leadership and governance. Through its membership and partnerships with state municipal leagues, NLC serves as a resource and advocate for more than 19,000 cities and towns and more than 218 million Americans. NLC's Center for City Solutions provides research and analysis on key topics and trends important to cities and creative solutions to improve the quality of life in communities.

About the Authors
Kyle Funk, Program Specialist of City Solutions

Cooper Martin, Director of Sustainability & Solutions

Nicole DuPuis, former manager of the Urban Innovation program at NLC's Center for City Solutions

Alan Shark, the Executive Director and **Dale Bowen** is Managing Director, Public Technology Institute at CompTIA.

Acknowledgements
NLC is grateful for the guidance and review from the Public Technology Institute; Angelina Panettieri, Principal Associate for Technology and Communications, Federal Advocacy and John Manwell, Program Director for Information Technology at NLC; and Dan Lohrmann, Chief Security Officer & Chief Strategist at Security Mentor, Inc.

Table of Contents

Foreword

Many of us remember a time before technology permeated every aspect of life – including our local governments. Not so long ago, our communities ran on filing cabinets stuffed with documents, fax machines and paper public transit schedules. Our timecards and records were kept by hand, and resident engagement only happened in-person or over the phone.

Today, our communities have moved online. This change has made many aspects of modern life more efficient. But this digital revolution is happening quickly, often at a pace faster than we can keep up with. As a result, individuals and institutions alike have been left vulnerable to hackers and ransomware.

Every day in the United States, a local government is hacked. Since 2013, ransomware attacks have impacted at least 170 county, city, or state government systems. The damage can cost millions, but the loss of public trust and safety come at an even higher price.

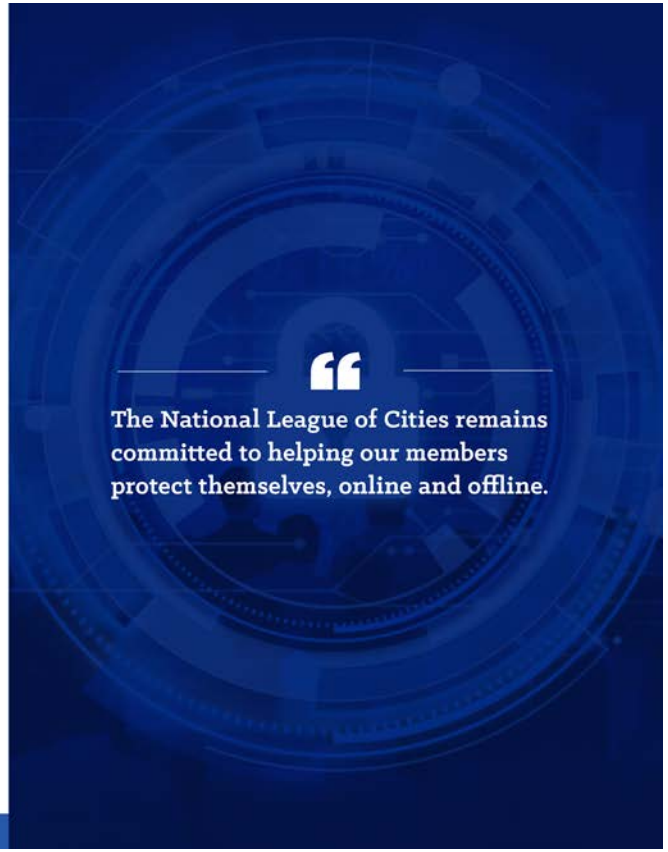
Despite being a primary target for hackers, local governments continue to integrate technology into their day-to-day operations and are increasingly collecting massive amounts of data. The pressure on cities to become "smarter" and more connected is mounting.

This rush toward digitization has resulted in a frenzy of competition and anxiety about being left behind, or not being able to provide the right services to their residents. As local leaders consider the risks and rewards of greater connection, they must also consider the crucial need for cybersecurity.

The National League of Cities remains committed to helping our members protect themselves, online and offline. That is why we are proud to release "Protecting Our Data: What Cities Should Know About Cybersecurity" in collaboration with the Public Technology Institute. This guide will help local leaders prepare and implement systems to protect their institutions online.

New technologies have the potential to create a brighter, more equitable future for the people in America's cities, towns and villages. But, cybersecurity and smart city initiatives must go hand-in-hand. If we continuously invest in the people and systems needed to keep our information secure, our communities will thrive.

Clarence E. Anthony
CEO and Executive Director, NLC



Introduction

The White House reported that there were 77,200 cyber incidents in 2015 occurring in federal agencies alone. The Federal Trade Commission (FTC) received more than 800,000 consumer fraud and identity theft complaints, where consumers reported losses from fraud of more than $1.2 billion. Security threats from the "outside" are increasing in frequency and sophistication, but most of the greatest threats are coming from users "within" – network users who click on malicious links, open email attachments that contain viruses, or make other mistakes that allow hackers to gain access.

Public services are going digital. At the most complex level, this requires policymakers to understand, manage and regulate the use of facial recognition software and micromobility technology like e-scooters, energy storage, smart energy meters or autonomous vehicles. But data is also increasingly at the core of more fundamental services such as trash collection, building and zoning permitting, fleet management, public facility operations, utility maintenance and even tree inventories. The pressure on cities to become "smarter" or more connected is mounting, resulting in a frenzy of competition and anxiety about being left behind. A report from the McKinsey Global Institute estimates that the economic impact of the internet of things (IoT) in smart cities could surpass $1.7 trillion worldwide in 2025.[i]

Local governments do not often think of themselves as tech organizations, but nearly everything a government does depends on its ability to create, maintain and share large quantities of data — and to ensure that data is secure. Undoubtedly, the confluence of government and technology has great potential for cities to improve service quality and efficiency. But embracing technology-driven governance is not without risk.

Today's networks are constantly being probed for weaknesses and vulnerabilities. All organizations must deal with these threats as technology continues to play a larger and larger role in business and governance. From Russia disrupting Ukraine's infrastructure and breaches of corporations such as Equifax and Marriott, to attackers targeting American cities like Atlanta, Baltimore, and Riviera Beach, FL, ransomware and email scams plague internet users daily.

Local leaders should make cybersecurity an administrative and budgetary priority. When a local government is the victim of an attack, the cost can far exceed that of proactive investment in cybersecurity. In 2016, the average cost of a data breach was estimated to be about $6.53 million.[ii] However, in many cities, the cost can be even higher, and the price of failing to secure our networks is clearly rising. The cost for Atlanta to recover from its ransomware attack was estimated around $17 million.[iii] Similarly, the recent Baltimore ransomware attack is predicted to cost over $18 million.[iv]

While there are several examples of high visibility hacks on the private sector, there are three main reasons why the concerns are very different when a local government falls victim to a breach:

- Governments collect and maintain far more sensitive information than most private sector companies.
- Residents can't easily move or choose a competitor if they are unhappy with their local government service and security.
- Trust in government is eroding, and security breaches may further reduce faith in government.

Cybersecurity and smart city initiatives must go hand in hand as local leaders continue to invest in 21st century infrastructure. This municipal action guide is a collaboration of the National League of Cities and the Public Technology Institute. Our aim is to strengthen cybersecurity policies and systems in local governments. The guide looks at the state of cybersecurity in local governments and includes policy recommendations for local leaders to implement in order to keep their residents, and their own data, safe. To get a clearer picture of the state of cybersecurity in local governments today, NLC and PTI conducted a small survey of PTI's IT members and NLC's Information Technology Committee (ITC). We found that while local governments are making improvements, they still lack support from elected leaders and face budget constraints that limit their abilities to improve cybersecurity further.

There are many simple and effective steps cities can take to avoid vulnerabilities and reinforce cybersecurity best practices:

- Identify one individual to be responsible for cybersecurity programs in that jurisdiction
- Make digital hygiene an institutional priority
- Educate the local workforce, elected leaders and residents about cybersecurity
- Conduct an analysis of local government vulnerabilities
- Ensure your data is properly backed up
- Implement multi-factor authentication
- Create policies or plans to manage potential attacks
- Ensure public communication is part of your attack response plan
- Adopt a dot gov (.gov) address to reduce risk of fraudulent municipal websites
- Work with educational partners to create a cybersecurity talent pool

No network can be 100 percent secure, but by following the recommendations in this guide, local government leaders can reduce the risk of a cyber-attack and be more resilient when one does occur.

What is Cybersecurity?

DEFINITIONS YOU SHOULD KNOW

CYBERSECURITY
The protection, confidentiality, integrity and availability of data, systems and infrastructure in technology. Cybersecurity is a combination of secure systems (hardware and software) built into technology as well as human intervention, monitoring, training, awareness, and good network habits.

MALWARE
Short for "malicious software," this software is designed specifically to damage or disrupt a system, such as a virus.

RANSOMWARE
A type of malware that threatens to publish or block access to data until a ransom is paid

BREACH
An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party

PHISHING
The illegal practice of sending email claiming to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and social security numbers

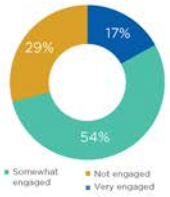
How Prepared are Cities?

NLC and PTI conducted a survey of IT officials representing local governments from across the United States to prepare for this survey. PTI sent the survey out to their broader membership while NLC targeted members of our Information, Technology and Communications Advocacy Committee, generating 165 responses:

45% represent communities with a population under **50,000**
33% represent local governments in the **50,000 to 150,000** population range
22% represent local governments **above 150,000** in population.

HOW ENGAGED ARE YOUR LOCAL OFFICIALS IN CYBERSECURITY EFFORTS?

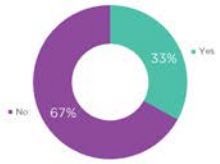
Only 17 percent of respondents say their local elected officials are very engaged in cybersecurity efforts. In fact, 29 percent admitted that they were "not engaged" at all.



IS YOU BUDGET ADEQUATE ENOUGH TO SECURE THE NETWORK PROPERLY?

When asked if the local government's budget was adequate, 67 percent of respondents said it was high enough to secure the network properly.

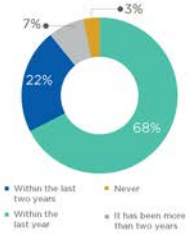
Over half of those who answered the survey said that elected officials tended not to prioritize cybersecurity budgets and policy.



DOES YOU LOCAL GOVERNMENT HAVE A CYBERSECURITY PLAN/STRATEGY?

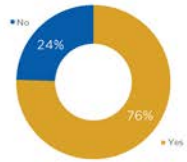
Over three-fourths (75%) of local governments have a cybersecurity plan/strategy in case of an attack. These plans also include the steps to recover data should the system be breached.

IF YOU HAVE A CYBERSECURITY PLAN, HOW OFTEN IS IT REVIEWED?

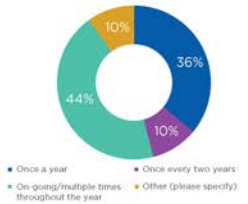


However, only 68 percent of these plans have been reviewed in the last year. This is troubling, since annual audits are considered a best practice with ever-changing technology and threats.

DOES YOUR JURISDICTION PROVIDE FOR EMPLOYEE AWARENESS TRAINING (WHAT TO DO AND WHAT NOT TO DO WHEN IT COMES TO CYBER SECURITY)?



IF YES, WHAT IS THE FREQUENCY?



PTI and NLC's survey revealed that around 76 percent of respondents conduct employee awareness trainings. While most (80%) conduct these trainings yearly, a few local governments only conduct cybersecurity training at employee onboarding.

The information collected by NLC and PTI are consistent with prior research and analyses in local government cybersecurity, indicating that little progress is being made to improve security in the face of mounting threats. In 2016, the International City/County Management Association (ICMA) and the University of Maryland, Baltimore County, conducted the first-ever survey of U.S. local governments about their cybersecurity practices and experiences. Their results revealed an alarming state of unawareness and unpreparedness for the majority of the 3,423 local governments they surveyed. These risks may cost local governments significant money and time as they seek to reverse the effects of a cybersecurity incident.

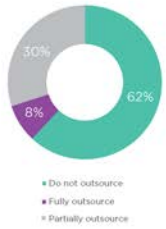
The most alarming result from the survey dispels the myth that cities, towns and villages are safe from attacks by bad actors. The survey found that 44 percent of local governments report an attack from a cyber incident hourly (26 percent) or daily (18 percent). That number rises to 66.7 percent over the duration of a year. But what is even more alarming is the large number of local governments that do not know how often they are attacked (27.6 percent), experience an incident (29.7 percent) or a breach (41.0 percent).

Worse still, while 88.8 percent of local governments know that most incidents come from external actors, nearly one-third (31.9 percent) do not know if the attacks were from an internal source or an external one. Even though local governments constantly experience incidents, a majority do not catalog or count attacks (53.6 percent).[9]

According to the ICMA/Univeristy of Maryland, Baltimore County survey, local governments are trying to improve cybersecurity resilience through policy planning. The top policies that governments adopted included rules regarding how passwords are created, requirements on the frequency that end users must change their passwords and use of employee personal electronic devices on local government systems. Even though these policies were adopted, most officials incorrectly wrote them off as ineffective to increasing cybersecurity.[10] The experts also noted in the paper that maintaining a strong cybersecurity culture with all users was vitally important. A strong cybersecurity culture means keeping good digital hygiene on top of mind, and sharing responsibility between all end users — not just the IT department or officials.

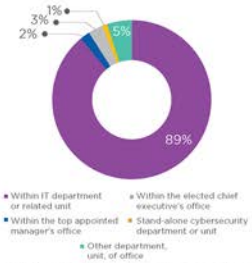
Though the ICMA/University of Maryland, Baltimore County survey revealed alarming cybersecurity results, the NLC/PTI survey shows that local governments are starting to adjust to the dangers the cyberworld presents. Three years have passed since the two surveys and cities, towns and villages seem to be progressing on cybersecurity. However, bad actors have not sat idly by. Nowadays, cybersecurity work will require constant evolution and local governments are best adapted to prepare and innovate solutions that can help the whole country remain secure.

DOES YOUR LOCAL GOVERNMENT OUTSOURCE ANY OF ITS CYBERSECURITY FUNCTIONS?



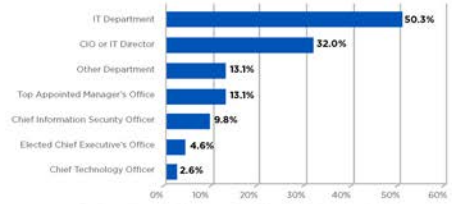
Graph courtesy of ICMA/University of Maryland, Baltimore County

WHERE IS THE PRIMARY RESPONSIBLY FOR CYBERSECURITY LOCATED IN YOUR LOCAL GOVERNMENT'S ORGANIZATION?



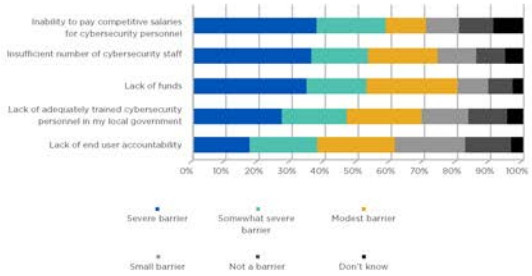
Graph courtesy of ICMA/University of Maryland, Baltimore County

IF OUTSOURCED, TO WHAT OFFICE OR OFFICIAL IN YOUR LOCAL GOVERNMENT DOES THE CONTRACTOR(S) TO WHOM YOU OUTSOURCE CYBERSECURITY REPORT?



Graph courtesy of ICMA/University of Maryland, Baltimore County

TO WHAT EXTENT IS EACH OF THE FOLLOWING A BARRIER FOR YOUR LOCAL GOVERNMENT TO ACHIEVE THE HIGHEST POSSIBLE LEVEL CYBERSECURITY?



Graph courtesy of ICMA/University of Maryland, Baltimore County

Private Sector Perspectives:

6 STRATEGIES FOR CYBER SECURE CITIES

Haiyan Song, Senior VP and GM, Security Markets, Splunk

Cities are increasingly focused on cybersecurity best practices, with several high-profile attacks in recent years causing major disruptions to city operations across our nation. Developing the practices and tools to protect our cities from ransomware, cryptomining and a wide range of emerging threats is vital to safety, data protection and the security of the critical infrastructure that cities manage. But there's hope in the chaos. The ability to dramatically improve your cybersecurity defense is within reach for the largest cities and smallest towns, provided we work together across all levels of government, academia and private sector partners.

Last fall I was honored to host a cybersecurity roundtable with the National League of Cities at Splunk's San Francisco headquarters, where I shared advice from my years of conversations with cybersecurity experts around the globe in every industry. Here are some of our observations:

1 **CITY LEADERS NEED TO UNDERSTAND THAT CYBERSECURITY ISN'T JUST AN IT DEPARTMENT CHALLENGE.** It's the responsibility of the entire organization, and the buck ultimately stops with leadership. In the private sector, there's no question that cybersecurity is now a CEO and board-level responsibility, and recent cyber incidents for local governments have made it clear that mayors, city managers and councilmembers must be informed and ready to lead on this issue. City leaders need to align with their IT and security staff and stay informed about cyber risks and their potential impact to the city.

2 **CITIES NEED TO START IMPROVING THEIR DEFENSES AND KEEP MOVING.** There is no "finish line" when it comes to cybersecurity. It's a continuous journey. No matter where your city is in its cybersecurity defense maturity, it's important to commit to always moving forward. Threats are always evolving, which means your strategy to monitor, detect and act on risks must as well. Has your city adopted a risk-based cybersecurity framework, such as the one from the National Institute for Standards and Technology (NIST)? Does your city have a cyber incident response plan? If so, how often is it tested?

3 **CYBERSECURITY IS A TEAM SPORT.** Just as cities proactively form partnerships to prepare for natural disasters, it is critical that cities forge strong partnerships for cybersecurity incident response before disaster hits. Even the most technologically mature cities will struggle with resources if they are hit with a major cybersecurity incident. Cities must play an active role in sharing and collaborating with each other, other levels of government and security industry partners.

4 **CITIES NEED TO UNDERSTAND THAT THE CYBERSECURITY TALENT GAP IS A GLOBAL PROBLEM WITH MILLIONS OF UNFILLED POSITIONS,** and everyone is scrambling to recruit and train the next generation of cyber defenders. Do your local universities, community colleges or high schools have cybersecurity programs? Identify both short- and long-term talent pipelines for cybersecurity in your region. Be a champion of these programs and your cities will benefit.

5 **BUDGETS ARE IMPORTANT.** City IT leaders have been red flagging cybersecurity and the lack of an adequate budget as their top priority for years. Does your city have a dedicated cybersecurity budget? Is that budget realistic to provide the protection you're aiming for?

6 **LASTLY, THERE'S AN IMPORTANT QUESTION ALL LOCAL GOVERNMENTS SHOULD ASK: DOES YOUR IT LEADERSHIP HAVE ACCESS TO THE MODERN TOOLS IT NEEDS TO DO ITS JOB EFFECTIVELY?** A modern cybersecurity practice fundamentally comes down to being smarter with data than those looking to do you harm or hold your data for ransom. Big data analytics, machine learning and even artificial intelligence (AI) aren't futuristic fantasies, they're the core technologies of today's cybersecurity defenses.

It's paramount that all city leaders look at security as a mission enabler and not just a checkbox. The most advanced cities I come across understand that data needs to be at the heart of any security operations center (SOC). And there's a hidden pot of gold in putting advanced data analytics at the center of your security strategy. We've seen countless enterprises that learned the modern skills of being "data driven" through their cybersecurity practices, and then transformed their organizations by transferring those skills into their core missions. There are even examples of organizations taking the data skills and machine learning tools they use for cybersecurity and applying them to pressing policy issues like combating the opioid crisis and human trafficking.

Policy Landscape and Resources for Local Governments

Cities are not alone in this effort to secure public information. Several state governments are stepping up to assist cities as they identify areas of cybersecurity vulnerability. Local leaders should be aware of what their own state might offer, and advocate for programs that have been successful from other state governments.

Examples of this work can be found in Georgia and West Virginia, which are cultivating state government ecosystems to help cities improve their cybersecurity defenses. Georgia offers consultations to all municipalities upon request. They do this by creating IT contracts that allow them to work for local governments for general purpose or incident response needs.[vii] West Virginia has also followed this route, setting up state contracts to allow local governments to take advantage of state resources.[viii]

New York and Virginia are attempting to help local governments with different approaches. New York's Department of Homeland Security and Emergency Services is helping local governments evaluate their vulnerability assessments against the Cybersecurity Framework developed by NIST. Virginia, on the other hand, is tackling cybersecurity with help from the military. The state has mobilized its National Guard to 'State Active Duty' status to perform vulnerability assessments and penetration tests on local government networks. The Commonwealth also plans to use homeland security grants to hold regional working group meetings on cybersecurity.[ix]

For any cybersecurity program to work, sharing costs and retaining talented cybersecurity employees in local governments is crucial. State officials in Michigan launched a chief information security office (CISO) service to aid nine small- and medium-sized governments. The program allows local governments to pay a fraction of the price for a trusted cybersecurity expert to assist them with their cybersecurity needs. CISO and other tech officials are engaged through this cost-sharing system which allows them to receive the expertise they normally could not afford on their own. This partnership approach resulted in improved cybersecurity for the state and was cited by FEMA as being a valuable example for other jurisdictions.[x]

Dozens of state and local government agencies are members of the Multi-State Information Sharing & Analysis Center (MS-ISAC). This coalition is open and free for all state, local, tribal and territorial governments. MS-ISAC is hosted by the non-profit Center for internet Security and supported by the Department of Homeland Security, and provides multiple resources, including a 24/7 Security Operations Center, Incident Response Services and a Vulnerability Management Program.

Cyber Disruption Response Plans

Every government must be prepared to respond to cyber emergencies, in the same way that fire departments train and prepare to respond to fires. The National Governors Association (NGA) has created guidance on how to respond to emergency cybersecurity incidents. The NGA publication examines 'Cyber Disruption Response Plans' across America and offers best practices and tips to help. Bottom line, every government should test their processes and procedures with business leaders at least annually with a tabletop exercise that addresses cyber and other threats.

-Dan Lohrmann, Chief Security Officer & Chief Strategist, Security Mentor, Inc., former leader of Michigan state government cybersecurity teams.

Local Government Examples

Durham, North Carolina

(228,330 population)

Durham, North Carolina, was hit with two major cyberattacks in the last decade. The first attack, in 2009, targeted the public-school system and multiple systems managing student grades, phones and other networks were down for three months. Once the systems were back online, over 5,000 teachers had to manually reenter grades and other information. In addition to the costs of restoring or replacing hardware, the attack reduced functionality of the school system for months and it took thousands of hours to recover information.

Thus, the city of Durham worked diligently to create new policies, procedures and plans to make sure an attack like the 2009 incident never happened again. The school district and elected leaders established a cyber security framework complete with context, leadership, evaluation, compliance, audit, review and media plan. They also established partnerships with the FBI, the state of North Carolina and MS-ISAC.

When a second attack occurred in 2018, the city was better prepared. This time, the fleet vehicle network was inflicted with a virus that tried to jump to other agencies. DeWayne Kendall, deputy director of technology Solutions for the city of Durham, was worried.

"We were on our way to being in the newspaper," he said.

When the second attack took place, staff quickly reached out to partners at MS-ISAC, who then connected them with staff in Allentown, Pennsylvania, who just had a similar attack. This time, instead of taking months to diagnose and identify the attack, they were able to do it in hours. The attack was shut down completely and the city was able to eliminate reinfections of the system within two weeks.

Worcester, Massachusetts

(Population estimate: 185,877)

The city of Worcester, Massachusetts, recognized that in order for its cybersecurity awareness program to be effective and successful, it must have support at the highest level. The city has increased its security efforts over the past year by prioritizing them in the fiscal 2019 budget, and creating a full-time data security specialist position to implement policies and procedures that will help safeguard the city's data. The city also created a cybersecurity awareness trainer position, another full-time employee whose job was to deliver cybersecurity awareness training to employees on an ongoing basis. The city started its cybersecurity awareness program in October 2018.

Since cybersecurity is too broad of an area to tackle all at once, city officials identified training as the first priority. They aimed to train employees on cybersecurity awareness and equip them with the knowledge to help identify and prevent cybercrime. Additionally, the city continues to

research cybersecurity best practices and available training for local government. To date, the city's cybersecurity awareness program includes:
A one-hour, mandatory introduction to cybersecurity awareness class to employees;

1. A process to encourage users to report suspicious emails;
2. Acknowledgement of "cyber champions" in each department who can help their co-workers identify "fake" emails, distribute awareness flyers and posters and participate in monthly meetings to provide input for additional cybersecurity awareness training;
3. Development and enforcement of security policies and
4. Creation of a cybersecurity incident response plan.

Cities interested in bolstering their approach to cybersecurity preparedness often start by seeking grant opportunities to help fund cybersecurity risk assessments. The city of Worcester received such funding to review current policies, processes and procedures and identify potential security risks.

Matanuska-Susitna Borough, Alaska

(Population around 100,000)

The Matanuska-Susitna Borough (Mat-Su) is a local government in Alaska with a population of about 103,000. Borough officials felt that they had a fairly secure system. The borough monitored web, email, and network traffic; weathered DDOS attacks, viruses, malware, and ransomware; and had a good backup/disaster recovery system designed to withstand the next big Alaska Earthquake.

In mid-2018, several local and state government organizations in Alaska were hit by cyber attacks. Matanuska-Susitna was hit with an advanced malware suite on July 23, 2018, that took down 150 servers and nearly 600 desktop computers. Mat-Su and the nearby city of Valdez were completely incapacitated. Both governments were infected with ransomware, but each responded differently. Valdez decided to pay the ransom, whereas Mat-Su did not. Upon investigation, Mat-Su found that the attack had infected and encrypted their backups. Primary cleanup and mitigation took three months and cost $2.5 million. To reduce the risk of a new infection, both locations completely rebuilt their networks and scrubbed all data imported to the new networks.

As for ransomware, the Mat-Su subscribes to the conventional wisdom of never paying a ransom, as doing so simply encourages the attacker to use new and bolder methods, and paying never guarantees a return of assets.

There are many models for cybersecurity, and the most common, *prevention*, is no longer enough. Since the attack, the municipality's multi-level email filters capture more than 650,000 bad emails an hour, and yet there are still dozens of targeted email attacks that get through daily. For prevention to work, a city's defense has to be correct 99 percent of the time, as no system will ever be perfect. Mat-Su now uses the *detect and contain* approach for that reason.

National League of Cities

The National League of Cities suffered a ransomware attack in February 2017. The total downtime experienced was less than 15 hours thanks to the inclusion of cybersecurity in NLC's disaster recovery plan. By having, following and sticking to the plan, NLC was able to recover the stolen files without having to pay the ransom.

One evening, a network user noticed that several files were locked on the network drive and suspected that this was a potential ransomware attack. They immediately called NLC's IT director who confirmed that the files were in a state of encryption caused by a ransomware attacker. The managed services provider (MSP) who maintains NLC's network was contacted and quickly discovered the attack was coming from an account logged on through a terminal network that allows for remote working — essentially, the attacker was posing as an NLC employee. They immediately disconnected the user and reset the password to stop the hacker from getting back into the network.

By that time, over 11,000 files had been locked by the attack. However, there was no need to pay the ransom because NLC backs up its data every night. The first thing NLC's disaster plan calls for is a recovery via a shadow copy from the off-site location to the on-site location, but this failed because of inadequate free space. A second action called for making the off-site file server the primary file server for the time being while the MSP took time to wipe clean and re-build the on-file server from scratch. Additionally, it was decided that terminal services be terminated during the recovery period and was later rebuilt.

There is nothing like an attack to test the disaster recovery plan for any government or organization, and NLC learned several important lessons about its strengths and vulnerabilities. First, the rapid response plan and nightly file backups allowed the organization to quickly respond to the initial attack. Second, hosting those backup copies off-site allowed the organization to quickly restore critical services after the attack, even while the primary file server was being rebuilt. Third, there were additional steps that the NLC could take to prevent similar attacks in the future. This included lengthening employee passwords to a minimum of 14 characters as suggested by the NIST security standard, adding an application to strengthen the terminal services by limiting the number of invalid login attempts, and implementing multi-factor authentication (MFA) on the terminal service and VPN. Finally, NLC made cybersecurity training mandatory for all staff with a focus on phishing and scams.

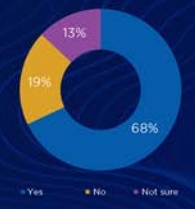
What Cities Need to Know About Cyber Insurance

As cyberattacks against local governments have become more widespread, cyber insurance has emerged as an attractive backup for some cities to expand the full set of cybersecurity protections. Insurance should not be considered an alternative to updating systems and improving digital hygiene, but no system can be 100% safe in such a dynamic and changing environment.

Cyber insurance premiums can cost thousands of dollars, but they can save a municipality much more, in the event that there is a cyberattack. Here are just a few things cities should include when thinking about the scope of potential coverage:

- Overtime for employees attempting to restore a system
- The cost of lost revenue (some non-recoverable)
- The cost of outside technical support servicesThe monthly and annual costs to provide "free" credit monitoring reports to affected citizens or businesses whose information was stolen
- The replacement of some equipmentLegal fees
- Forensics after an attack occursCrisis management and post-event related expenses

DOES YOUR LOCAL GOVERNMENT CURRENTLY HAVE CYBER INSURANCE?



IF YES, WHAT IS THE COVERAGE AMOUNT?

WHAT DO CYBER INSURANCE COMPANIES LOOK FOR?

Some cyber insurance forms ask dozens of key questions. Failure to answer honestly could lead to a denial of payment. Imagine a chain smoker who smokes ten packs a day and falsely claims to be a non-smoker on a medical insurance form. Were the patient to succumb to a smoking-related illness, the insurance company is not obligated to pay anything. In the cyber realm, those providing cyber insurance want to minimize their risk as well, and premiums and deductibles are predicated on how good your jurisdiction manages its digital infrastructure. Common questions are:

- Has the jurisdiction adopted a cybersecurity incident response plan and adopted basic technology practices and policies?
- Are internet and email use policies reviewed with employees, elected leaders and contractors?
- Are employee access rights reviewed?
- How often is employee training provided and what is addressed?
- How are backups of devices managed?
- What anti-spam, anti-virus filters, anti-malware are utilized?
- Is computer access terminated when an employee departs?
- Is there an on-going process of forcing employees to change passwords?
- Are service providers required to demonstrate adequate security policies and procedures?
- What are the security and privacy provisions for cloud and managed services?
- What procedures are in place to test or audit your policies, procedures and controls?

PTI's and NLC's national survey of local government information technology officials revealed that 70 percent of respondents have cyber insurance. However, when asked what the amount of their insurance coverage was, 50 percent of respondents "did not know." Whether known or not, the amount of coverage and exposure should be reviewed on a regular basis to make sure your organization is properly covered. While cyber insurance does not protect your municipality from a cyber-attack or breach, it does help to mitigate the risk that your municipality could be crippled indefinitely by an attack or faced with the prospect of having to front thousands of even millions of dollars in the wake of a cyber event. With this in mind, cyber insurance should be considered a key component of your government's cybersecurity strategy.

Finally, be sure to reach out to your state municipal league to determine whether they offer cyber insurance through their affiliated risk pools.

Strategies and Recommendations for Local Leaders

1. **Identify one individual to be responsible for cybersecurity programs in that jurisdiction**
   This individual should be the "go-to" person when a security problem arises, and also serve as an "ambassador" who promotes cybersecurity awareness within the organization. With this role, they can also serve to enforce your cybersecurity rules and ensure staff receive the necessary training. They should report directly to the local government's top executive/administrator. Larger municipalities should hire a full time IT executive. For smaller jurisdictions with tight resources, hiring a full-time IT person to help with more complex issues may not be possible. This is when local governments should consider soliciting state/county resources or partnering with a neighboring jurisdiction to address this need.
2. **Make digital hygiene an institutional priority**
   For local elected officials, keeping residents safe and secure is no longer just about having an able police force and sound justice system. Today, security encompasses the digital world and ensuring bad global actors cannot take advantage of weaknesses in online systems. Local leaders should work to promote a shift toward cybersecurity as a governing priority, both internally and in their connected communities. This should include emphasizing the importance of cybersecurity in the city budget, instituting best practices around cybersecurity and digital hygiene, recruiting new staff with cybersecurity and technical skills, training existing staff annually, training new staff as part of onboarding, and conducting an audit to identify points of weakness within local government networks.
3. **Educate the local workforce, elected leaders, and residents about cybersecurity**
   While investing in sophisticated software is important, towns and villages should take, investing heavily in people is also critical. NLC and PTI recommend that cybersecurity awareness training happen at least once a year, if not more. All new staff, including newly elected officials, should receive cybersecurity training as part of their onboarding processes. Lastly, periodic awareness campaigns should occur throughout the year. Be sure to also think what role city hall can play in reaching out to small and medium size business and schools. These places are also under constant attack. At the annual National Night Out in 2018, the city of Bellevue, Washington, created a venue for IT staff and community relations coordinators to meet with neighborhood groups, residents of low-income housing units and other local groups to inform parents and their children about online safety. The team plans to return next year and even started a monthly newsletter.
4. **Conduct an analysis of local government vulnerabilities**
   Before making any significant investments in cybersecurity systems or reinforcements, it is valuable to assess the gaps and weaknesses in your local government's network. For

This is a rapidly changing landscape and there is an ongoing up-tick in attack vectors which make this a topic that cannot be ignored. Staff must know how to protect the enterprise systems and perimeter while balancing security and functionality. This requires an advanced, ever-evolving skillset and the ability to communicate and train end users rapidly. This is not just an IT problem, but an organizational one.

-Chris J. Neves, IT Director, City of Louisville, Colorado Information Technology

local governments, this might include identifying any vulnerabilities present in connected infrastructure throughout the city. Simple tabletop exercises for officials to practice their incident response plan can help identify these vulnerabilities, and many state governments can help coordinate these drills. As noted above, MS-ISAC is supported by the federal government to help local governments analysis and recommendations.

5. **Ensure your data is properly backed up**
   The number one defense against ransomware is tested, offline (non-connected or cloud hosted) backups. This is an extension of good digital hygiene that is worth emphasizing for its own sake. Even organizations that have policy in place need to ensure that backups are being conducted frequently, that these backups are sufficiently isolated to avoid attack, and that they are technically capable of restoring service and functionality.

6. **Implement multi-factor authentication**
   Multi-factor authentication (MFA) is a valuable tool against attacks. MFA requires a user to enter an additional security code or confirmation via their smartphone, e.g., through an app or text message. Cities should implement MFA on all business-critical systems, e.g., email. If an attacker gained the credentials of a city employee through a phishing attack, the attacker would still be blocked from gaining access because they don't have their employee's smartphone.

7. **Create policies or plans to manage potential attacks**
   Every local government should have a cybersecurity response plan. This can be developed internally or with the help of a private sector firm that specializes in security. The plan should include several key components:

   - Employee awareness training, incident response and after-action planning.
   - An incident response team, similar to ones created to address natural or man-made disasters.
   - Protocols to notify local law enforcement as well as other appropriate officials (state officials, the US Department of Homeland Security, FBI). Almost all states require that local governments contact the state CIO, the state attorney general, and other departments.
   - Prioritization of systems to restore in case of an attack. For most governments this would mean making sure safety and health services come back online first or a shifting of resources if services cannot be brought back on immediately

8. **Ensure public communication is part of your attack response plan**
   Public trust is essential to local government, and when it comes to potential attacks, public communication is a unique concern.

   Utilize all of your jurisdiction's communications channels to share information with the public – the press, social media, television. In the event of a data breach, some state laws require the local government to notify the press if a certain number of personally identifiable pieces of information are exposed.

   What should you tell the public? Your community needs to know that their local leaders are fully engaged in the situation and are working to resolve it. To maintain the public trust, it is important to be as transparent as possible, keeping in mind that your jurisdiction is involved in a situation that impacts the public safety and full details may not be available until after the situation is resolved.

9. **Consider converting to a dot gov (.gov) domain**
   Hackers are not only attempting to target cities, they may impersonate a municipal service in order to target your residents. Identity thieves can easily create websites in the dot com (.com) or dot org (.org) domains that can look and seem like a legitimate web page and direct targets there to pay bills or submit personal information. These scams can be reduced by establishing your municipal systems on a .gov domain, which is much more difficult to mimic.

10. **Work with education partners to create a cybersecurity talent pool**
    Individuals with cybersecurity skills are highly sought after in today's job market, and the public sector often struggles to compete with the higher salaries in the private sector. Local leaders should tap into local community colleges, universities and high schools to help fill cybersecurity gaps. This way students can get hands-on experience and serve their communities, which may encourage to stay in in those positions. Two examples of this already exist. For twenty years, Cisco Networking Academy has worked to help students gain technical and entrepreneurial skills. Students can take courses online in subjects such as the IoT and cybersecurity. Along the way, Cisco will help students seek out job and networking opportunities. CompTIA is also working to create certifications around cybersecurity and keep those in the IT world on a growing path throughout their careers.

Conclusion

Today, digitization of services and management of sensitive data requires cities to invest in cybersecurity to fend off risks to their network. Local governments are in the midst of a sea of change, as more and more of their basic governance functions rely on technology. Connected infrastructure is critical to service delivery and efficiency.

Many improvements to local cybersecurity will involve partnerships between cities and private consultants or vendors who can provide important services. It is essential that local leaders understand that they can outsource many of these functions, but they cannot outsource responsibility. They have a duty to embrace cybersecurity both in practice and policy as tech is integrated into our cities, towns and villages. Local governments can prepare by doing the cyber basics and then begin stepping it up from there. Local elected officials owe it to their residents to protect their most valuable data — it is their responsibility, their duty of care. The National League of Cities and the Public Technology Institute stand ready to help the nation's local governments strengthen their cybersecurity efforts.

Local elected officials owe it to their residents to protect their most valuable data — it is their responsibility, their duty of care.

References

NLC/PTI Survey: NLC and PTI conducted a survey of IT officials representing local governments from across the United States to prepare for this survey. PTI set the survey out to their members while NLC sent the survey out to it's ITC Committee. With 165 responses 45 percent represent communities with a population under 50,000, 33 percent represent local governments in the 50,000 to 150,000 population range while 22 percent represent local governments above 150,000 in population.

Label Resources

What the Public Knows About Cybersecurity (Pew Research Center) https://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Americans and Cybersecurity (Pew Research Center) https://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf

Cyber Resilience: Digitally Empowering Cities (J. Paul Nicholas, Jim Pinter, et al., Microsoft) https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW6auc

Cybersecurity And The Rise Of Smart City Vulnerability (Smart Resilient Cities) https://www.smartresilient.com/cybersecurity-and-rise-smart-city-vulnerability

Cybersecurity: Protecting Local Government Digital Resources (Microsoft and ICMA) https://icma.org/sites/default/files/18-038%2520Cybersecurity-Report-hyperlinks-small-109617.pdf

Cybersecurity Challenges to American Local Governments (Donald F. Norris et al., UMBC) https://ebiquity.umbc.edu/_file_directory_/papers/874.pdf

Cybersecurity: A Necessary pillar of Smart Cities https://web.archive.org/web/20180218234603/http://www.ey.com/BI/Publication/vwLUAssets/ey-cyber-security-a-necessary-pillar-of-smart-cities/$FILE/ey-cyber-security-a-necessary-pillar-of-smart-cities.pdf

The Dangers of Smart City Hacking (IBM) https://public.dhe.ibm.com/common/ssi/ecm/75/en/75018475usen/final-smart-cities-whitepaper_75018475USEN.pdf

MS-ISAC https://www.cisecurity.org/ms-isac/

National Cybersecurity Preparedness Consortium http://nationalcpc.org/

National Cyber Security Alliance https://staysafeonline.org/

National Institute of Standards' Cyber Security Framework https://www.nist.gov/cyberframework

End Notes

1. Unlocking the Potential of the Internet of Things, by James Manyika and al. 2015. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world
2. Barker, "The Economic Costs of Being Hacked," BetaNews, BetaNews, Inc., February 10, 2016. http://betanews.com/2016/02/10/the-economic-cost-of-being-hacked/
3. Deere Stephen. Confidential Report: Atlanta's cyber attack could cost taxpayers $17 million. *The Atlanta Journal-Constitution*. August 2018.
4. Duncan, Ian. Baltimore estimated cost of ransomware attack at $18.2 million as government begins to restore email accounts. *Baltimore Sun*. May 29, 2019.
5. Cybersecurity: Protecting Local Government Digital Resources by Corey Fleming and all. ICMA and Microsoft, May 2017.
6. Ibd.
7. Cohen, Natasha. Cyber Incident Response and Resiliency in Cities: How Partnerships Can be a Force Multiplier. *New America*. February 2019.
8. Ibd.
9. Ibd.
10. Lesson Learned: Cybersecurity: The Michigan Cyber Disruption Response Strategy

Appendix A: Cybersecurity Checklist

The following is a comprehensive checklist to determine the level of security controls within your city.
This checklist was adapted from a resource developed by James E. Pacanowski II, CGCIO, Ventnor City, N.J.

Physical Security		
Item	**Yes**	**No**
Do you have policies and procedures to address authorized and limited access to facilities, including data centers?		
Are visitors escorted in and out of controlled areas?		
Are PC screens automatically locked after an idle period?		
Do you have policies covering laptop, tablet, or mobile device security?		
Do you have a current emergency evacuation plan?		
Do you have an accurate up to date inventory of all electronic equipment?		
Are your data closets and/or server rooms equipped with intrusion alarms?		
Is your data center/server room locked at all times?		
Do you have environmental controls dedicated to your data closets and server rooms?		
Do you have fire suppression systems dedicated to your data closets and server rooms?		
Are default security settings changed on software and hardware before they are placed in operation?		
Are policies and procedures in place to control equipment plugged into the network?		
Is your physical facility monitored and reviewed via camera systems?		
	Totals	

Personnel		
Item	**Yes**	**No**
Does your staff wear ID badges?		
Do you check credentials of external contractors?		
Do you have policies to address background checks of contractors?		
Do you have policies addressing background checks of employees?		
Do you have a policy for unauthorized use of "open" computers?		
Do you have a policy and procedure in place to handle the removal of employees who retire, are terminated, or leave, including passwords and access to systems?		
Do you have an acceptable use policy that governs email and internet access?		
Do you have a policy governing social media use and access by employees?		
Are employees required to sign an agreement verifying they have read and understood all policies and procedures?		
Are these policies and procedures reviewed by employees at least annually?		
Totals		

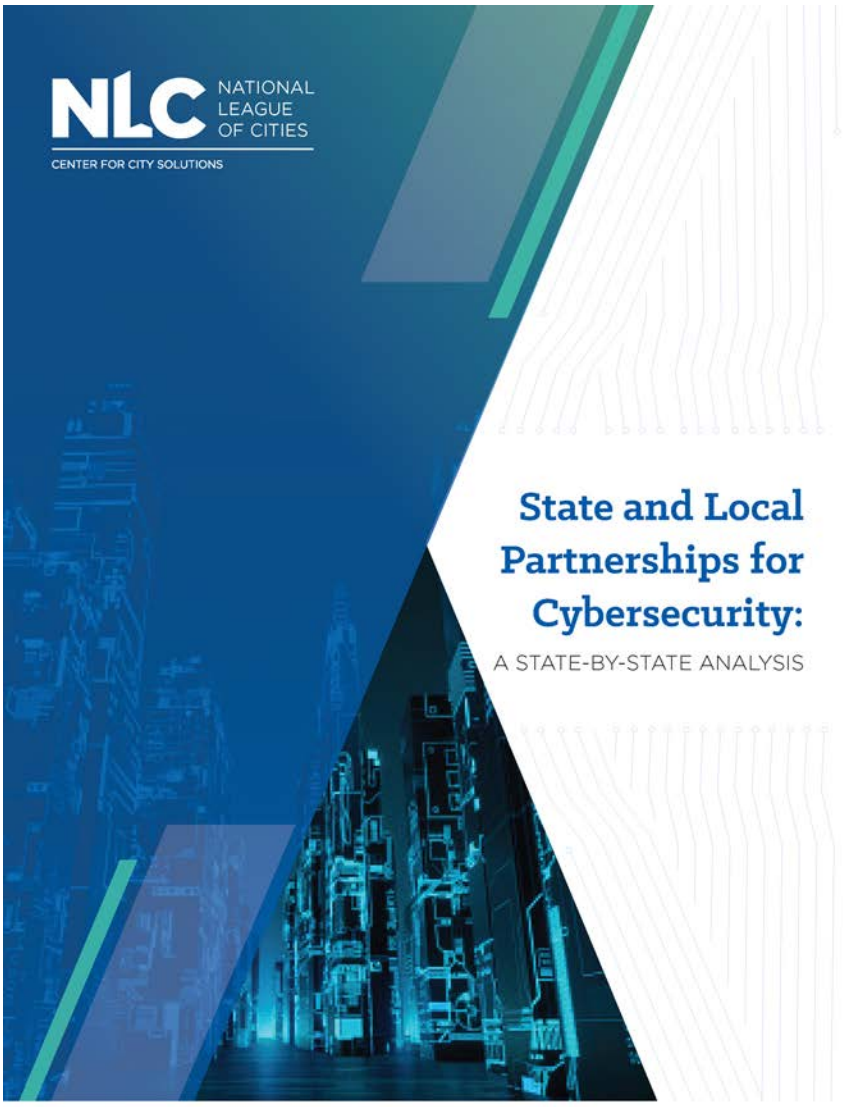
Account and Password Management		
Item	**Yes**	**No**
Do you have policies and procedures covering authentication, authorization, and access control of personnel and resources to systems?		
Are policies in place to ensure only authorized users have access to PCs?		
Are policies and procedures in place to enforce secure, appropriate, and complex passwords?		
Are information systems such as servers, routers, and switches protected with basic or better authentication mechanism?		
Has the default "Administrator" account been disabled and/or deactivated?		
Are all access attempts logged and reviewed?		
Are employees required to change their passwords on a routine schedule?		
Are employees prevented from using previous passwords?		
Are all passwords on network devices encrypted?		
Do you have legal and/or policy notifications on all log-in screens that is seen and accepted prior to access to any network device?		
Totals		

Data Security		
Item	**Yes**	**No**
Do you have policy for information retention?		
Do you have policies and procedures for management of personal private information?		
Do you have a policy for disposing of old and outdated equipment?		
Do you have policies and procedures in place for the secure destruction or sanitation of media and/or drives before they are removed, sold, or disposed of?		
Is access to data or systems accessed remotely both from a dedicated link and encrypted?		
Do you have policies and procedures in place to ensure that documents are converted into formats that cannot be easily modified before they are circulated outside the network?		
Are documents digitally signed when they are converted to formats that cannot be easily modified?		
Is access to critical applications restricted to only those who need access?		
Are UPS batteries used on all critical equipment?		
Totals		

Network Security		
Item	**Yes**	**No**
Is network traffic regularly monitored for patterns?		
Do critical systems have redundant communication connections?		
Does your network utilize redundant DNS servers in case of interruption to one server?		
Are your DNS servers reviewed on a periodic basis for anomalies and consistency?		
Is your Active Directory reviewed periodically for anomalies and consistency?		
Are all unnecessary services disabled on servers?		
Does your network utilize redundant domain controllers in case of interruption to one server?		
Are there policies and procedures governing the use of wireless connections to your network?		
Are wired and wireless networks within your organization segregated either physically or virtually through routers, switches, or firewalls?		
Do you employ firewalls on your network to control access and traffic?		
Are firewalls configured to only allow traffic from approved lists?		
Are network security logs reviewed regularly?		
Are web filters used to restrict downloading of unapproved material?		
Are filters or firewalls used to filter executable or malicious email attachments?		
Are policies and procedures in place for software patches and updates?		
Are policies and procedures in place for hardware patches and updates?		
Are your security policies reviewed on a yearly basis?		
Are current and up to date antivirus solutions loaded on all computers?		
Are antivirus and other security software updated with current patches on a regular basis?		
Do you use spyware and malware detection software?		
Are all computers current with all security and operating system patches and updates?		
Do you use employee "least privilege" access and review access privilege periodically?		
Do you have an accurate and up to date software inventory list?		
	Totals	

NLC NATIONAL LEAGUE OF CITIES

CITIES STRONG TOGETHER


NLC
NATIONAL
LEAGUE
OF CITIES
CENTER FOR CITY SOLUTIONS
State and Local Partnerships for Cybersecurity:
A STATE-BY-STATE ANALYSIS

NLC NATIONAL LEAGUE OF CITIES
CENTER FOR CITY SOLUTIONS

About the National League of Cities

The National League of Cities (NLC) is the voice of America's cities, towns and villages, representing more than 200 million people. NLC works to strengthen local leadership, influence federal policy and drive innovative solutions.

NLC's Center for City Solutions provides research and analysis on key topics and trends important to cities and creative solutions to improve the quality of life in communities.

About the Authors

Christiana K. McFarland is the Research Director of NLC's Center for City Solutions. **Brenna Rivett** is a program manager. **Kyle Funk** is a program specialist. **Rose Kim** is a program specialist, and **Spencer Wagner** is a program specialist in NLC's Center for City Solutions.

Acknowledgments

The authors would like to thank Laura Cofsky who edited the report, and Paris Williams who designed the report.

About the Report

This report is the sixth project outcome of a research collaborative between NLC and the state municipal leagues. We are grateful for the guidance, data verification and cybersecurity narratives they provided.

Table of Contents

Foreword

Much of our world has gone digital. In many communities, everything from paying utility bills and acquiring permits, to requesting sidewalk repairs and reporting potholes, is now done online. These changes have made many aspects of our daily lives more efficient. However, they come with a price.

Today, local governments are a major target for hackers, and they can cost cities millions. More importantly, these attacks threaten to erode the trust that residents have in critical institutions. Over the last few years, cities, towns and villages — as well as states — have launched pragmatic, creative solutions to defend themselves. But perhaps more importantly, both local and state governments are increasingly realizing that they can't shoulder the burden of cybersecurity alone. It's a team sport that requires everyone to work together, using strategies that play to everyone's strengths.

As we move into election season, it is crucial that we keep our communities secure and protect our democratic systems from bad actors. At this time, there is no roadmap, and states vary widely in the kinds of cybersecurity supports they currently offer. That's why my team and I at the National League of Cities have prioritized this issue and created resources that are both reliable and immediately applicable for the cities we serve.

To that end, we have surveyed the various ways that states are supporting cities in their cybersecurity efforts. *State and Local Partnerships for Cybersecurity: A State-By-State Analysis* is meant to help local governments better understand best practices for working with their state government, and what resources may already exist that they can tap.

We are stronger together. After reading this guide, I hope that leaders of cities, towns and villages, and the states in which they reside, will be able to forge ahead and build strong, resilient systems, both online and off, to protect their residents from cyberattacks.

Onward,

Clarence E. Anthony
CEO and Executive Director
National League of Cities

Introduction

On July 4th, 2019, the town of New Bedford, Massachusetts was hit with the largest local government cyberattack in history with a ransom demand of $5.3 million. Despite the significant ransomware attack on a town of less than 100,000 people, the overall effect was muted due "to a combination of luck — at the time of attack, most devices were still turned off for the July 4 holiday — and an IT architecture that compartmentalizes several key city departments, including police, schools and utilities."[1] As a result of the city's preparations, only four percent of computers were affected and no city services were disrupted.

This incident underscores that cyberattacks can hit any community at any time, regardless of size. While many cities are not prepared, those that have cybersecurity efforts in place benefit greatly. Cybersecurity refers to the protection, confidentiality, integrity and availability of data, systems and infrastructure in technology. Cybersecurity is a combination of secure systems (hardware and software) built into technology as well as human intervention, monitoring, training, awareness, and good network habits.

Despite the necessity, the reality is that many local governments are resource constrained and do not have dedicated funding for cybersecurity infrastructure or personnel. The good news, however, is that they don't have to face cybersecurity alone. State governments can be strong allies to local governments. They have greater access to financial and workforce resources and greater capacity to provide critical services.[2]

This guide outlines some of the most impactful ways that local governments can work with their state governments to prepare and defend again cyberattacks. Strategies discussed in this guide include:

- Mandatory breach reporting;
- State training initiatives;
- Cybersecurity Task Forces, Working Groups, and Councils;
- State and Local Shared Cybersecurity Services; and
- Non-Government Cybersecurity Partners.

The report also includes profiles of effective city-state partnerships from across the country. As cities, towns and villages continue to be on the frontlines of cyberattacks, a collaborative approach between cities and states, together with Federal and university partners, can lead to a stronger national cybersecurity infrastructure in the face of growing threats.

STATE AND LOCAL PARTNERSHIPS FOR CYBERSECURITY: A State-By-State Analysis

Mandatory Breach Reporting

Mandatory breach reporting is required in all 50 states and the District of Columbia. These laws require private and/or public entities to alert affected individuals of any security breaches involving personal data.[3] California was the first state to enact such a law in 2002. The most recent states to enact similar laws were Alabama and South Dakota in 2018.[4] Despite consensus that mandatory breach reporting is a critical cybersecurity strategy, there are vast differences in these laws from state to state. These differences are primarily based on the type of entities affected, the type of personal information involved, the manner in which the data were stolen and the requirements for notification — such as timing and other entities that should be alerted.[5]

Mandatory Breach Reporting Thresholds for Local Governments

Is there a threshold a people affected by a breach to triggers state notification? If so, how many people?

These laws also vary in their reporting requirements. 36 states require that municipalities report breaches to the state. Typically, municipalities are required to report to the state attorney general but depending on the state it can include the state insurance regulator or other entity.

Of the 50 states and the District of Columbia, the states can be classified as either 1) having no breach reporting requirement to the state government (14 states and the District of Columbia); 2) states that require notice regardless of the number of people affected by the breach, or no threshold (18); and 3) states that have a threshold for reporting (18).

No breach reporting requirement

Fourteen states and the District of Columbia require that entities notify affected individuals (as all states do), but do not require the entity to alert the state government or officers. These include states like Georgia and Minnesota.

Reporting requirement without a threshold

Eighteen of the 36 states do not have a threshold at which they have to notify the state; thus, municipalities must report a breach to the state no matter how many people are affected. Montana, New York and Wisconsin are examples of these states.

Reporting requirement with a threshold

The other 18 states have thresholds at which point they must notify the state government. For instance, Delaware requires a public entity to alert the state if 500 or more people are affected in a breach. New Mexico on the other hand requires notice to the state if 1,000 or more people are affected. There are three common thresholds: 250, 500 or 1,000 people.

- Four states require notice if at least 250 people are affected;
- Seven states require notice if at least 500 people are affected;
- Seven states require notice if at least 1,000 people are affected.

When alerting the state, some are required to provide not just the names and contact information of the individuals affected, but also a summary of the breach and services that have been or will be offered, such as in Florida and Alabama.

CASE STUDY:

Mandatory Breach Requirements in Alabama

One of the most recent states to adopt a mandatory breach requirement law was Alabama. According to the executive director of the Alabama League of Municipalities, Ken Smith, the recent law has not caused major headaches for cities and towns, as fortunately a major breach has not yet occurred.

"There will obviously be a problem trying to notify everybody, and we have been trying to get the word out through presentations and events," stated Smith.

He and league director of IT, Chuck Stephenson, traverse the state speaking about the law and other actions in the cybersecurity space. This represents just one proactive approach the state and the League have taken when confronting cybersecurity. In 2020, there will be regional training sessions in the state to highlight the resources available to municipalities, including The Multi-State Information Sharing & Analysis Center (MS-ISAC) and the League's cybersecurity partner, Sophicity.

Smith reiterated, "One of the biggest results that came about from some of the legislation like this was just a realization that we all needed to be a little bit more aware of it and take steps and try to prevent cyberattacks as much as we possibly can."

STATE AND LOCAL PARTNERSHIPS FOR CYBERSECURITY: A State-By-State Analysis

State Training Initiatives

As the number of cyberattacks continues to grow each year, governments assume significant, unforeseen financial losses. To address vulnerabilities and raise awareness, states have offered various types of cybersecurity training initiatives for government employees, including local governments, to protect against future incidents. Of the states that offer cybersecurity training initiatives, most governments have mandatory or voluntary trainings for state employees. Regardless of whether local government employees currently have access to these programs, it's helpful for them to be aware that they exist and to explore how to build partnerships.

Voluntary for State Employees

Currently, 22 states (Alabama, Arizona, Arkansas, California, Connecticut, Iowa, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Mississippi, New Jersey, New York, North Carolina, Oklahoma, Rhode Island, South Carolina, South Dakota, Tennessee, Utah and Wisconsin) offer voluntary cybersecurity training programs for state employees. Common resources states offer to employees include online cybersecurity training videos, toolkits and in-person classes through partnerships with postsecondary education institutions.

Trainings take many forms. The Arkansas Division of Information Systems has developed an online cybersecurity toolkit to promote cybersecurity awareness in a practical and entertaining way. The toolkit includes factsheets, guides and webinars for state government employees to utilize. Meanwhile, the Connecticut Department of Administrative Services partnered with Connecticut community colleges to offer non-IT personnel in-service courses in cybersecurity awareness. Finally, the state of Iowa's Information Security Division provides online services for state employees to utilize, such as cybersecurity education training videos, anti-malware tools, wipe utility programs, and storage and file protection programs.

Voluntary for Local Employees

Delaware is the only state that offers voluntary statewide cybersecurity training for state non-executive and local government employees. For state executive branch agencies, however, the state of Delaware requires formalized annual employee cybersecurity awareness training.

Mandatory for State Employees

Sixteen states (Colorado, Florida, Georgia, Illinois, Louisiana, Maryland, Montana, Nebraska, Nevada, New Hampshire, Ohio, Oregon, Pennsylvania, Vermont, Virginia and West Virginia) require formalized cybersecurity training programs for their state employees. In Pennsylvania, the Office of Administration's Information Technology Department developed a cybersecurity program for state agencies that includes access to antivirus software and web-based security awareness trainings on cybersecurity best practices. Similarly, Illinois' Department of Innovation and Technology has a mandatory annual online cybersecurity training course for state employees that covers phishing scams, spyware infections and identity theft, and data breaches.

Mandatory for Local Employees

In 2019, Texas passed a law that requires most state and local government employees to formalize cybersecurity trainings for their employees. Under House Bill (HB) 3834 of the 86th Texas Legislature, the Texas Department of Information Resources, in partnership with the Texas Cybersecurity Council, will be required to develop and implement a certified cybersecurity training program to state government employees that perform at least 25 percent of their duties using a computer, local government employees with access to a municipal computer system or database, elected and appointed officials, and state government contractors.[6]

Public-Private Partnership

Wyoming is the only state that established a public-private partnership to implement a state employee cybersecurity training program.

No State Training Initiative

There are nine states (Alaska, Hawaii, Idaho, Indiana, Kansas, Missouri, New Mexico, North Dakota and Washington[7]) that do not have any type of state or local government cybersecurity training program.

Although most states offer cybersecurity training programs to state-level government employees, it could be cost-effective to also grant local governments access to these cybersecurity services online and free of charge. Furthermore, as most of these resources address common cybersecurity risks that affect both state and local governments, such an initiative could encourage knowledge-sharing between different levels of government.

STATE AND LOCAL PARTNERSHIPS FOR CYBERSECURITY: A State-By-State Analysis

CASE STUDY:

Local Cybersecurity Initiatives in Michigan

Michigan has been at the forefront of developing an effective cybersecurity ecosystem model. The state is implementing innovative solutions to educate government employees on cybersecurity protection measures, improve overall awareness on cyber-related issues and prepare for future cyberattacks.

Although Michigan's voluntary cybersecurity training program is offered to state-level government employees, Michigan's state government has collaborated with local partners to develop voluntary tools to improve cybersecurity education and preparedness within the state. One type of local collaborative effort with the state includes support from five Michigan counties: Livingston, Monroe, Oakland, Washtenaw and Wayne. This partnership was successful in the development of CySAFE, a free IT security assessment tool to "help small and mid-sized governments assess, understand and prioritize their basic IT security needs."[8]

Another innovative solution was the launch of the Michigan Cyber Range in the city of Ann Arbor in November 2012. The program provides "secure cybersecurity training, research and exercise environment for IT security professionals" in educational institutions, private businesses and the public sector — including local governments.[9] The purpose of this initiative is to enhance Michigan's protection of computer systems and sensitive data through hands-on cybersecurity awareness trainings and simulation exercises.[10]

In recent years, Michigan has become one of the few state leaders in prioritizing and implementing effective state government cybersecurity measures through leadership, innovation and strong collaboration. It's essential for states to recognize the urgency of complex cybersecurity issues and develop effective cybersecurity measures to prepare for potential cyber threats in the future.

STATE AND LOCAL PARTNERSHIPS FOR CYBERSECURITY: A State-By-State Analysis

Cybersecurity Task Forces, Working Groups and Councils

Over the last few years, 25 states have established cybersecurity task forces, working groups and councils. The vast majority of these states, seventeen, created these groups through an executive order, while the other seven created the groups through legislation. One state, Maryland, utilized both an executive order and a bill to establish its cybersecurity council.[9]

From a city perspective, these groups are important because they often contribute to, or define, state policies on cybersecurity, including influencing what offerings are available to local government. In the long-term, accessing these groups could be an effective first step in times of crisis. In Massachusetts, the working group includes cities as official members, providing strong linkages across sectors and various levels of government.[12]

State-Level Cybersecurity Task Forces, Working Groups or Councils

These groups serve a variety of purposes: For states that are newer to cybersecurity, they can provide an opportunity to start those conversations, while for others they create a platform for continuing discussions and policies. Unlike long-established sub-committees such as transportation and finance, cybersecurity is a relatively new arena for state and local governments, and it is not yet widely represented at state capitals. Task forces, working groups and councils are therefore important mechanisms for governments to implement policies and procedures to protect themselves and residents from cyberattacks.

The landscape of these groups varies widely from state to state. Some states establish them for a set amount of time to achieve key goals[13,14], others set them up as ongoing convenings of key personnel to address present and future issues[15,16], and several use them as temporary measures to conduct research or produce reports.[17]

When it comes to cybersecurity task forces, working groups and councils, states fall into one of three categories:

- The state has a working group, task force or council established by executive order (17 states)
- The state has a working group, task force or council established through legislation (7 states)
- The state has a working group, task force, or council established first by legislation and then an executive order (1 state)
- The state does not have an established group working on cybersecurity (25 states and the District of Columbia)

CASE STUDY:

Kansas City, MO: A Regional Approach to Tackling Cybersecurity

One example of a state-level cybersecurity council can be seen in Kansas City. The Kansas Information Technology Security Council created numerous resources for local governments and cities to utilize.[18] Additionally, working with the Center for Internet Security (CIS), MS-ISAC and the Mid-Atlantic Regional Council, Kansas City formed a Regional Cybersecurity Strategic Framework with a goal to "create a shared service model to support local governments."[19]

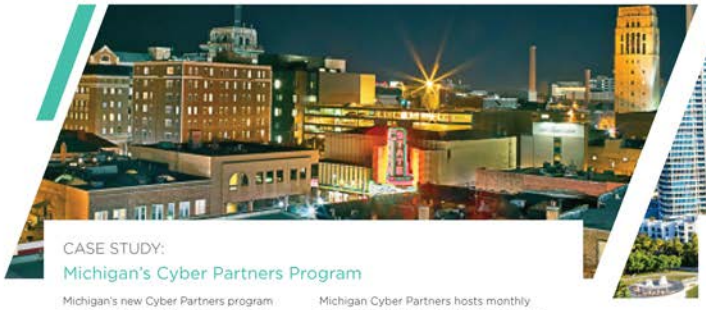
The effort started with a simple goal: to improve cyber hygiene for all communities in the region, regardless of size. Representatives from cities and counties, IT specialists and other cybersecurity experts worked together to develop the regional framework. They established benchmarks and best practices that centered around resiliency and redundancy. This regional approach is especially helpful for small cities that may not have the capacity on their own to audit their systems and upgrade accordingly. The approach also offers flexibility so that agencies that already have an effective framework are not forced to change. The CIO of Overland Park, Kansas, Tony Sage, says "one of the biggest strengths of the program is that it's based on a really collaborative approach."

State and Local Shared Cybersecurity Services

Local governments often come together with other governments to bundle purchases or to share services such as water treatment and delivery. Taking this shared approach for cybersecurity can help solve some of the critical barriers facing local governments, including budget constraints and personnel training. One approach is "inter-governmental sharing" of cybersecurity services.[20] It can include shared service agreements for cyber defense tools, IT/CIO shared staff or regional cybersecurity defense centers.

Although most states across the country do not have a dedicated state and local shared cybersecurity service, Idaho, Illinois, Michigan and Texas have created programs that others can learn from. Idaho's is currently getting ready to launch and others like Michigan and Illinois, are only in certain areas.

But cities, towns and villages cannot create this shift alone. States can help lead in this space. At a minimum, states should be building relationships with local governments and raising awareness of existing services. States can provide resources like staff or cybersecurity infrastructure to local governments. They can also play the more traditional role of providing technical assistance in the form of startup grants and loans for shared capital projects that deal with cybersecurity shared programs. States can also gather key stakeholders to enable shared cybersecurity services. Lastly, they can lower barriers by creating incentives for both the private and public realms to partner on cybersecurity programming.



CASE STUDY:

Michigan's Cyber Partners Program

Michigan's new Cyber Partners program is rebooting the state's successful Chief Information Security Officer (CISO) as a service program with a state-wide vision that includes a community approach to prevention, preparation and incident response. For two years, the state of Michigan piloted it's "CISO as a Service Program." During 2017 and 2018, thirteen communities received services from a CISO-level consultant who conducted a local cybersecurity assessment and assisted in developing a remediation plan. There were monthly teleconferences where all participants discussed assessment results, lessons learned and overall program development. The smallest community to use the program was Springfield, Michigan (pop. 13,000), which has only one full-time IT employee, and the largest was Washtenaw County (pop. 360,000).

Michigan Cyber Partners hosts monthly state-wide Skype meetings that highlight current cyber threats, discuss mitigation strategies related to the threats and provide a deeper dive on important topics. Additionally, cyber incident response is provided by the Michigan State Police Cyber Command Center and the Michigan Cyber Civilian Corps. Currently, Michigan is making plans to reintroduce the program as a public-private partnership in order to expand the program out to the rest of the state.

STATE AND LOCAL PARTNERSHIPS FOR CYBERSECURITY: A State-By-State Analysis

CASE STUDY:

Florida Innovation in the Cyber Space

The Florida League of Cities created a new grant program through the Florida Municipal Insurance Trust (FMIT) that helps local governments combat the ever-growing threat of ransomware attacks. The grant pays for cloud-managed backup services for up to two servers, along with one terabyte of backup space for each participating member. If a local government experiences a ransomware attack, its data is securely backed up in the cloud and can easily be restored, so the local government won't feel pressured to pay a ransom. The grant covers the total cost of managed backup services for the first year, and half for years two and three. After the third year, the local government takes full ownership of backing up its environment. Funding for the grant is provided through the FMIT, and the program is run by the Florida League of Cities.

"Our goal is to ensure that FMIT members understand that backing up their most sensitive and important data is a key defense against a cyberattack," said Michael van Zwieten, director of technology services for the Florida League of Cities. "The FMIT Data Recovery Grant Program gives members the tools to secure their data and make it retrievable through a managed-service partnership."

Launched in early 2020, the Data Recovery Grant Program is available to FMIT members with property and liability coverage.

Government in Michigan, like many states, is diverse, distributed, and interconnected. From a cybersecurity perspective, we present a broad attack surface to our adversaries. The response to this challenge can only be pulled together and address our common challenge with collective action. Michigan Cyber Partners provides the umbrella under which we'll do this.

Andy Brush
Cybersecurity Partnerships at the State of Michigan Department of Technology, Management and Budget

ELECTION SECURITY AND CITIES

At the time of this writing, the 2020 primaries and presidential election are top of mind for many cybersecurity experts. For city leaders, understanding the landscape of election security is crucial so that votes are kept safe and confidential. According to election security experts, there are three main levels of election security that are important to understand:

1. NATIONAL VOTER REGISTRATION DATABASE. This list contains information on all Americans registered to vote and can be accessed by the federal, state and local governments. Keeping this list accurate and secure is imperative, but also presents a challenge since there are multiple access points with varying levels of security.

2. BALLOT CREATION. If the computer that creates the ballots is directly or indirectly connected to the internet, it can be infected with malware.[23] This level of security is often the most overlooked.

3. BALLOT BOX. It is also the hardest to track, because every state and county can utilize different systems. Most states and counties are moving back toward paper voting, and away from electronic voting, which is more susceptible to hacks and security threats. But it is still a work in progress because changing the ballot type is expensive and time consuming.[25]

City leaders can work with county and state election officials to protect and safeguard the democratic process. The National League of Cities will be releasing a report later this year solely focused on local-county partnerships on this topic.

State Approaches to Cybersecurity

One of the biggest challenges in strengthening cybersecurity is that cities are often unaware of available resources at the state and national levels. Below are snapshots from four states that are representative of the diverse options available to local governments. These four state examples are meant to showcase the variety of ways that states are tackling cybersecurity and highlight new avenues that local governments can consider tapping into. The representatives from these states all had a common message for local governments: Collaboration is key. Local governments, counties, states and federal agencies all need to work together to address cyber threats, and that can look different in each state or region.

WISCONSIN

Number of Programs: 4

Type: National Guard Partnership and State Agency Programs: Defensive Cyber Operations Element, Cyber Protect Team and Wisconsin Statewide Intelligence Center

The state of Wisconsin has mobilized to build out a robust slate of services for local governments. Wisconsin, through its Department of Military Affairs, utilizes the Wisconsin National Guard to run analytics for local governments. The Defensive Cyber Operations Element (DCOE) is composed of 10 personnel who can help establish a baseline of "security, through analytics and system forensics." There is also the Cyber Protection Team (CPT) that focuses

THE MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER

Every state in the country has access to the Multi-State Information Sharing and Analysis Center (MS-ISAC) which runs under the Center on Internet Security (CIS). MS-ISAC is a free service designed to help the nation's overall cybersecurity efforts. Every state also has at least one, if not more, Fusion Center which, under the Department of Homeland Security, deals with coordinated threat protection and emergency responses. Leveraging and partnering with both of these organizations at the local and state levels could be crucial to securing municipalities around the country.

exclusively on cyber operations and threat emulation. The Wisconsin Department of Justice has created the Wisconsin Statewide Intelligence Center (WSIC), which is a fusion center for the sharing of threat-related information between state, local, territorial, federal and private sector partners. The WSIC offers a variety of products and tools for its partners, including analytic reports, malware analysis and cyber liaison officer training.

FLORIDA

Number of Programs: 1

Type: University Partnership

The state of Florida has created The Florida Center for Cybersecurity (Cyber Florida) which is built on the three pillars of education and workforce development, innovative research, and outreach and engagement.[24] Cyber Florida is hosted at the University of South Florida and works with all 12 State Universities, industry, government and defense to be a national leader in cybersecurity.[25] There is also ongoing discussion in the state legislature to consider funding Cyber Florida so it can provide matching grants to local governments to enhance technology infrastructure, employee training and technology audits. Another proposed piece of legislation aims to provide open records protection for technology-related information that might leave local governments vulnerable to cyberattacks/ransoms.

PENNSYLVANIA

Number of Programs: 1

Type: National Guard Partnership

The state of Pennsylvania has one of the strongest cybersecurity programs for county government that has yet to be extended to municipalities, known as PA Cybersafe.[26] The only resource the state of Pennsylvania offers for cities, town and villages is to help them connect with national organizations (MS-ISAC, National Council of ISACs and the Government Technology Institute Security Center of Excellence).

UTAH

Number of Programs: 4

Type: State Agency Program, Fusion Center, National Guard Partnership, and University Partnership

Utah takes a multi-faceted approach to cybersecurity. They partner with local universities to give students the opportunity to work on real-time cybersecurity projects and are in the process of finalizing a partnership with the Utah National Guard to aid in responding to cybersecurity issues. The state has also set up a Fusion Center, through the Utah Department of Public Safety, which brings together disparate levels of government and experts from a variety of fields to efficiently and effectively tackle cybersecurity threats and attacks.[27] In the past, Utah offered cybersecurity training to local officials, but the funding for those trainings has dried up and the state is currently looking for other funding sources.

Non-Government Cybersecurity Partners

University Partners

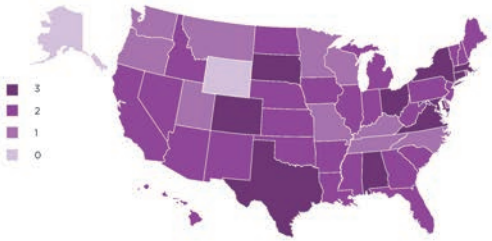
State governments have long partnered with their public or private two- and four-year universities to address critical issues in their states, from aligning talent with business needs and providing extension services, to, more recently, bolstering cybersecurity at the state and local levels. These partnerships are usually created by including a line item in the state budget that sends money to one of these post-primary education places to build a program. Strong university programs can not only help develop the cyber and IT public sector pipeline but also manage and protect data, respond to cyberattacks, offer cybersecurity training and convene critical stakeholders.

Most states (30) have created an official partnership with universities and colleges for cybersecurity-related support and services. For example, the state of Idaho partners with the SANS Institute, Girls Go CyberStart and Cyber FastTrack to identify talented youth who may be able to fill cybersecurity professional needs. Two Idaho undergraduate students won $22,000 through the Cyber FastTrack program to get a certificate in Applied Cybersecurity from the Sans Institute.[28]

The federal government, through the National Security Agency (NSA) and the Department of Homeland Security (DHS), sponsors two-year, four-year and graduate level institutions in National Centers of

Partnerships: Higher-ed, CAE Cyber Defense and CAE Cyber Operation

How many types of partnerships does each state have?



Academic Excellence (CAE) in Cyber Defense. According to CAE in Cyber Defense, "the goal of this program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise."[29] There are currently 272 total institutions throughout forty eight states with accredited universities. Only Alaska and Wyoming do not have an accredited place of higher learning. While there is no DHS funding for CAE Cyber Defense schools, some funding opportunities exist through the National Science Foundation. This system can be reworked to help local governments strengthen their cybersecurity capabilities.

The NSA also designates Centers of Academic Excellence in Cyber Operations. The program supports the President's National Initiative for Cybersecurity Education (NICE) which seeks to build a digital nation and a skilled workforce capable of supporting a cyber-secure nation. Currently, there are 16 states with a college or university holding this designation. While this program is deeply technical, it may be a source for states to tap into as technology continues to evolve.

National Guard Partners

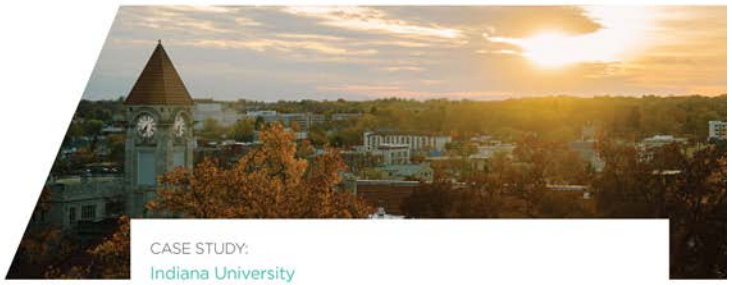
In addition to university partners, states have turned to their National Guards as a resource to defend against cyber-related attacks, safeguard information assets and protect the "digital and physical infrastructures" of localities.[30]

In total, the National Guard has "nearly 4,000 service members dedicated to cybersecurity across 59 units in 38 states and anticipates adding more through 2022."[31] Although every state has its own National Guard agency, some state cyber response units are responsible for covering multiple states. For example, the Army National Guard's 91st Cyber Brigade is based in Virginia but oversees cyber units in 30 states.[32] Within the 91st Cyber Brigade, there are only four states (Indiana, Massachusetts,

State Cybersecurity National Guard Partnerships

Does the state have a cyber response unit?

STATE AND LOCAL PARTNERSHIPS FOR CYBERSECURITY: A State-By-State Analysis



CASE STUDY:

Indiana University

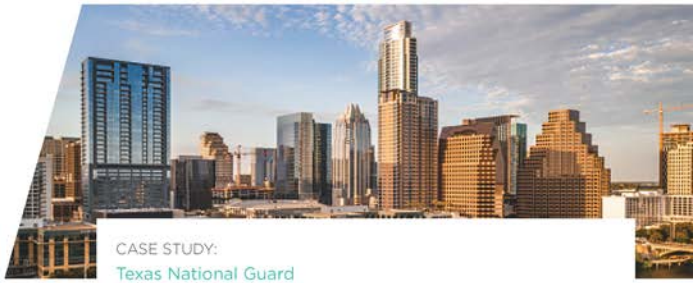
For 20 years, Indiana University (IU) has been at the forefront of universities that help manage cyber risk, has established an IU Cybersecurity Clinic to serve as a hub for Midwest cyber training needs. It will address threats faced by businesses, individuals, and state and local governments. Funding for the work comes from a grant foundation and matching funds of up to $225,000 from the Indiana Economic Development Corporation. The clinic will bring together businesses, law, informatics, computing and engineering school students to help state and local government agencies better manage cyberattacks, protect intellectual property and improve privacy. Through the clinic, IU hopes to continue Indiana's focus on supporting multidisciplinary innovation across the state. Academic director of the IU Cybersecurity Clinic Scott Shackelford is thrilled, "to train the next generation of cybersecurity professionals while helping to protect people and organizations around the globe, starting with our communities right here in Indiana."[33]

South Carolina and Virginia) that have a total of five cyber battalions in the National Guard (Virginia has two cyber battalions). In addition to responding to and neutralizing cyberattacks, members in the battalion will provide other types of support. For instance, the newest cyber battalion in Indiana will "offer cybersecurity expertise to companies, provide training readiness oversight to conduct cyberspace operations, network vulnerability assessments, security cooperation partnerships, and FEMA support along with cyberspace support of federal requirements."[34]

The National Guard has also implemented the Cyber Mission Assurance Team (CMAT), a new type of cyber response unit, in three states (Hawaii, Ohio and Washington). The purpose of this pilot program is to check federal facilities that rely on the state's critical infrastructure services. In 2014, the CMAT in Washington state conducted a utility grid assessment in the Snohomish County Public Utilities District to address vulnerabilities. Additionally, the Washington CMAT supported election security systems as they provided additional cybersecurity to ensure secure elections.

Finally, the National Guard has developed and activated eleven Cyber Protection Teams (CPTs) across 24 states (Alabama, Arkansas, California, Colorado, Georgia, Illinois, Indiana, Kentucky, Louisiana, Maryland, Michigan, Minnesota, Mississippi, Missouri, Nebraska, New Jersey, New York, North Dakota, Ohio, South Dakota, Tennessee, Texas, Utah and Wisconsin).[35] CPTs provide cyber defense capabilities across all levels of government, which includes "incident response, vulnerability assessments, network and host-based analysis and threat emulation."[36]

The National Guard's mission has evolved to play a crucial role in providing effective cybersecurity support and assistance across all levels of government. This includes the development and deployment of various types of cyber units to respond and defend against cybersecurity threats in a timely manner. In the long term, continuing to develop and activate new types of cyber response units is a cost-efficient and practical option for state and local governments.



CASE STUDY:

Texas National Guard

In 2019, a ransomware virus attacked local computer systems in Jackson County, Texas. Digital services in the public sector, such as property transfers and police background checks, were disrupted. The Texas National Guard's Cyber Incident Response Team was deployed to assess the ransomware attack and work with the county's IT system to restore local network operations.

Later, in a coordinated cyberattack, 23 small Texas towns were hacked and held for ransom. Due to the experience from the ransomware attack in Jackson County earlier that year, the state responded immediately, deploying multiple agencies and resolving the attack in two weeks, without having to pay the hackers. The National Guard's role in this attack was crucial once again because it was able to perform an assessment of the attack and prevent further damage.

Concerned by the growing cyberattacks, the Texas Military Department, the "umbrella agency for the state's National Guard branches," invited state, local and county officials to demonstrate how the Texas National Guard's Cyber Incident Response Team plans to prepare for future cyberattacks on different government agencies.[37] In addition, the Texas Military Department provided information for local officials to improve their awareness on cybersecurity and advised localities on ways to protect local networks.

Hackers are increasingly targeting state, county and local governments nationwide. Small, local governments are especially vulnerable to ransomware viruses as they lack the financial resources and expertise. It's important for states to support vulnerable local governments to prepare and utilize the National Guard as an available resource to defend against cyberattacks.

STATE AND LOCAL PARTNERSHIPS FOR CYBERSECURITY: A State-By-State Analysis

Conclusion

Many cities, towns and villages remain vulnerable to cyber threats from global actors. Given their resource constraints, collaboration with their state government is proving to be a viable path forward.

Almost every state has implemented mandatory breach reporting, created state executive training initiatives and brought in non-state partners like universities and the National Guard to strengthen cybersecurity. Yet, work remains to be done in areas like election security, trainings at the city and county level, local autonomy, and state and local shared services.

To better bridge the gaps between state and local governments, consider implementing these key recommendations:

1. Build relationships with local governments: Every local government should have a point person on cybersecurity. State governments can start by identifying who that contact person is and reaching out to them. Having a strong state-city relationship is also important so that states are better positioned to support local governments. State municipal leagues are a great starting resource for building these relationships.
2. Raise awareness of existing services: A big hurdle for local governments is finding out what services exist for local municipalities at the state level. State governments can help by marketing these services or programs to localities. Annual gatherings could also help to fill the void and promote new and existing programs.
3. Update and create official policy for today's threats: In today's evolving cybersecurity world, states and cities need to make concerted efforts to partner and work together, rather than embrace a top-down approach. Creating new legislation on a new topic can be daunting, but legislators at both the state and local levels need to come together to create nimble policies that can be utilized in a variety of cybersecurity situations.
4. Include local governments in service contracts: Sound policies are only as strong as the budgets behind them. Cost can be a burden for both state and local governments and raising taxes is difficult. It is important to think about programs that build across existing networks or contain shared services for multiple government entities.
5. Work with team players such as higher education, the National Guard and the private sector: Cybersecurity and defense are team sports. State governments can lead by bringing all the pertinent partners together, including municipalities, to build programs, connect resources and defend against attacks.

By exploring these paths, state and local governments can begin to build a strong patchwork of cybersecurity. Elected leaders at every level of government know cybersecurity is an issue that is not going away. As the problem grows in complexity, it is more crucial now than ever that local and state governments work together. Doing so will result in better solutions for employees, governments and, ultimately, the residents they serve.

Additional Resources:

MS-ISAC – Center for Internet Security: One of the best free programs out there that many state and local governments are using is the Multi-State Information Sharing & Analysis Center (MS-ISAC). This coalition is open and free for all state, local, tribal and territorial governments. MS-ISAC is hosted by the non-profit Center for internet Security and supported by the Department of Homeland Security, and provides multiple resources, including a 24/7 Security Operations Center, Incident Response Services and a Vulnerability Management Program. State governments should work with State Municipal Leagues to promote and make sure all local governments know that MS-ISAC exist. More information can be found here: https://www.cisecurity.org/ms-isac/ and a list of current local government participants can be found here: https://www.cisecurity.org/partners-local-government/

Fusions Centers: There are 79 Fusion Centers across the country. Find location and contact information here: https://www.dhs.gov/fusion-center-locations-and-contact-information

What the Public Knows About Cybersecurity (Pew Research Center): https://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Americans and Cybersecurity (Pew Research Center): https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Cyber Resilience: Digitally Empowering Cities (J. Paul Nicholas, Jim Pinter, et al., Microsoft): https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW6auc

Cybersecurity: Protecting Local Government Digital Resources (Microsoft and ICMA): https://icma.org/cyber-report

Cybersecurity Challenges to American Local Governments (Donald F. Norris et al., UMBC): https://ebiquity.umbc.edu/_file_directory_/papers/874.pdf

Cybersecurity: A Necessary pillar of Smart Cities: http://iranarze.ir/wp-content/uploads/2019/09/10116-English-IranArze.pdf

The Dangers of Smart City Hacking (IBM): https://public.dhe.ibm.com/common/ssi/ecm/75/en/75018475usen/final-smartcities-whitepaper_75018475USEN.pdf

National Cybersecurity Preparedness Consortium: http://nationalcpc.org/

National Cyber Security Alliance: https://staysafeonline.org/

Protecting Our Data: What Cities Should know about Cybersecurity: https://www.nlc.org/sites/default/files/2019-10/CS%20Cybersecurity%20Report%20Final_0.pdf

Endnotes

1 Freed, B. (2019, September). Ransomware demanded $5.3M from Massachusetts city in July attack. *StateScoop*. Retrieved from https://statescoop.com/ransomware-demanded-5-3m-from-massachusetts-city-in-july-attack/

2 National Association of State Chief Information Officers. (2019). *2019 State CIO Survey*. Retrieved from https://www.nascio.org/wp-content/uploads/2019/11/2019StateCIOSurvey.pdf

3 Greenberg, P. (2018). Security Breach Notification Laws. Retrieved from www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

4 Lazzarotti, J. J., et al. (2018, April 9). State Data Breach Notification Laws: Overview of the Patchwork. *Jackson Lewis*. Retrieved from www.jacksonlewis.com/publication/state-data-breach-notification-laws-overview-patchwork

5 BakerHostetler. *Data Breach Charts*. 2018, pp. 1-34.

6 Freed, B. (2019, September). Texas starts mandatory cybersecurity training for government employees. *StateScoop*. Retrieved from https://statescoop.com/texas-mandatory-cybersecurity-training-government-employees/

7 There is no public data or information available

8 Michigan Technology, Management and Budget Department. (2015). *Michigan Cyber Initiative 2015*. Retrieved from https://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_0115_2PM_web_474227_7.pdf

9 Ibid.

10 Mulholland, J. (2012, November). Michigan Launches 'Cyber Range' to Enhance Cybersecurity. *Government Technology*. Retrieved from https://www.govtech.com/Michigan-Launches-Cyber-Range-to-Enhance-Cybersecurity.html

11 Greenberg, P. (2019, September). Statewide Cybersecurity Task Forces. Retrieved from https://www.ncsl.org/research/telecommunications-and-information-technology/statewide-cybersecurity-task-forces636128887.aspx

12 Cyber Resilient Massachusetts Working Group. (n.d.). Retrieved from https://masscybercenter.org/cyber-resilient-massachusetts/cyber-resilient-massachusetts-working-group

13 Boshart, R. (2015, December). Iowa Governor Calls on Tech Leaders to Craft State Cybersecurity Strategy. Retrieved from https://www.govtech.com/security/Iowa-Governor-Calls-on-Tech-Leaders-to-Craft-State-Cybersecurity-Strategy.html?utm_source=relatedutm_medium=directutm_campaign=Iowa-Governor-Calls-on-Tech-Leaders-to-Craft-State-Cybersecurity-Strategy

14 Cybersecurity Task Force Action Plan. (2016, December). Retrieved from https://www.cybersecurity.mo.gov/files/task_force/plans/FINAL_Cybersecurity_Task_Force_Action_Plan_12.29.16.pdf

15 Gov. Hutchinson establishes computer science and cybersecurity task force. (2019, December 8). Retrieved from https://talkbusiness.net/2019/12/gov-hutchinson-establishes-computer-science-and-cybersecurity-task-force/

16 Montana Information Security Advisory Council. (n.d.). Retrieved from https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC

17 Currey, M., & Raymond, M. (2019, January 1). State of Connecticut 2018 Cybersecurity Update. Retrieved from https://portal.ct.gov/-/media/DAS/BEST/Security-Services/2018-Connecticut-Cybersecurity-Report.pdf?la=en

18 KISO Services. (n.d.). Retrieved from https://pts.ks.gov/kiso/Services

19 Cybersecurity. (n.d.). Retrieved from https://www.marc.org/Government/Cybersecurity

20 Kronos, J. D. (2019, January). The Role of Shared Services in Technology Investment. *Governing*. Retrieved from https://www.governing.com/topics/workforce/The-Role-of-Shared-Services-in-Technology-Investments.html

21 Access To and Use Of Voter Registration Lists. (2019). Retrieved from https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx

22 Shelley, K. and Williams, W. (2019, September). Election security isn't that hard. *Politico*. Retrieved from https://www.politico.com/agenda/story/2019/09/10/election-security-000954

23 Geller, E., et al. (2019, January). The scramble to secure America's voting machines. *Politico*. Retrieved from https://www.politico.com/interactives/2019/election-security-americas-voting-machines/

24 https://cyberflorida.org/

STATE AND LOCAL PARTNERSHIPS FOR CYBERSECURITY: A State-By-State Analysis

[26] About Cyber Florida. (2019). Retrieved from https://cyberflorida.org/about/

[27] Ward, M. and Brunner, M. (2020, January). Stronger Together: *State and Local Cybersecurity Collaboration*. Retrieved form https://www.nascio.org/wp-content/uploads/2020/01/NASCIO_NGA_StateLocalCollaboration.pdf

[28] Utah Department of Public Safety: Statewide Information & Analysis Center. (n.d.). Retrieved from https://siac.utah.gov/?_a=a2

[29] Hyer, M. H. (2019, November). Idaho continues partnership encouraging students to explore cybersecurity careers. Retrieved from https://gov.idaho.gov/pressrelease/idaho-continues-partnership-encouraging-students-to-explore-cybersecurity-careers/

[30] National Centers of Academic Excellence. (n.d.). Retrieved from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

[31] Ikeda, S. (2019, November). U.S. National Guard's Evolving Mission Includes Assisting Local Governments Experiencing Cyber Attacks. *CPO Magazine*. Retrieved from https://www.cpomagazine.com/cyber-security/u-s-national-guards-evolving-mission-includes-assisting-local-governments-experiencing-cyber-attacks/

[32] Ibid.

[33] Ibid.

[34] Wilkins, N. and Cook, K. (2019, July 2). First-of-its kind Cybersecurity Clinic to train 21st- century cyber professionals. *Indiana University*. Retrieved from https://news.iu.edu/stories/2019/07/iu/releases/02-cybersecurity-clinic.html

[35] Coble, S. (2019, November). Midwest to Get First Cyber Battalion. *Infosecurity Magazine*. Retrieved from https://www.infosecurity-magazine.com/news/midwest-to-get-first-cyber/

[36] Soucy, J. (2015, December 9). Guard set to activate additional cyber units. *National Guard Bureau*. Retrieved from https://www.nationalguard.mil/News/Article-View/Article/633547/guard-set-to-activate-additional-cyber-units/

[37] McClanahan, S. (2019, November 6). 169th Cyber Protection Team is capable and ready. *U.S. Army*. Retrieved from https://www.army.mil/article/229547/169th_cyber_protection_team_is_capable_and_ready

[38] Osbourne, H. (2019, October 29). State cyberteam helps agencies respond to uptick in ransomware attacks. *Statesman*. Retrieved from https://www.statesman.com/news/20191023/state-cyberteam-helps-agencies-respond-to-uptick-in-ransomware-attacks


NLC
NATIONAL
LEAGUE
OF CITIES
CENTER FOR CITY SOLUTIONS

SUNAPEE
SCHOOL DISTRICT

June 17, 2021

Sunapee School District's Written Testimony

To: The Senate Subcommittee on Emerging Threats and Spending Oversight

On October 21, 2019, after returning to work from a New Hampshire fall weekend, I received a call upon entering the District's office from the Director of Technology. He informed me that all our servers, documents and internal information structures had been locked down by an entity outside the District and that we were being asked to pay ransom for its release.

Sunapee is a small district in the western part of the state with 430 students (PreK-12) and 120 faculty/staff. The IT Department consists of one full time director and a technician who works 15 hours a week. Neither employee had the professional experience to prepare them to deal with or fully understand what had just happened.

We quickly called the local police department, state police, and our insurance carrier. Our first concern was for personally attributable student and staff information such as social security numbers, DOB and bank account information, but we had no immediate way to determine if that had been breached. Moving quickly, Primex, our local municipality insurance carrier, stepped in and put us in contact with professionals in computer forensics, data loss lawyers and computer specialists. With their assistance, we recognized that this was a ransom threat and determined that no data was taken but rather we were just blocked from accessing it. As this was going on, our focus quickly shifted towards the education of our students, and we began working with teachers to prepare them for what would turn out to be nine days without much of the technology they had become accustomed to using each day.

Working with our professional consultants, we made a determination that we could use our system backups done the Saturday prior. My 1.3-person tech department worked night and day to determine if any individual teacher or student machines may have been infected, removed and replaced servers and hard drives, made copies of our back up, and worked step by step through procedures while also trying to support the educational processes that needed to continue each school day.

At the conclusion of the nine days, we had accumulated fees, materials, and hardware totaling more than $40,000. This figure did not include the staff hours from our IT staff or the time teachers spent to recreate any content that may have been lost. While much of this was covered by our insurance carrier, the work completed and lost by district personnel was immeasurable. We were ultimately very fortunate, but the incident was not without cost.

Our primary goal in public schools is to provide educational opportunities for our students, and today so much of how we educate interacts with technology. Yet technology is still looked upon as a "set aside" department in most schools, as a place to reset your password when you forget it.

The overall budget for this District is twelve and a half million dollars a year, with approximately five hundred thousand dedicated to technology each year. In the aftermath of this event, the District invested $10,000 for a technology audit which was done by an in-state technology company that specializes in IT security and development. We now know that

SUNAPEE
SCHOOL DISTRICT

in an ideal world we should develop better systems to keep us fully protected in a crisis such as to develop a disaster recovery plan, write a business continuity plan, create redundant back-up systems that are offsite, enable multifactor authentication and train staff how to use it, run phishing drills to help educate students/staff on outside threats, and think about installing a dry sprinkler system in all IT closets holding technology equipment.

The audit also identified the need for additional support in our IT department. Our 1.3-person department works very hard each day to ensure that devices are in-hand, accessibility to needed information is available, equipment is ordered and repaired as needed, and helpdesk tickets are completed. The ability to research new technology and upgrade infrastructure systems is simply not possible given the capacity of the current staff. To add an additional full time person with benefits to our IT department would impact the budget by about 1 percent.

As a member of the American Association of School Administrators (AASA) and after completing their national certification program in February, 2020, I had the opportunity to discuss IT security with 20 colleagues from across our country. The cohort consisted of superintendents from districts in California, Pennsylvania, Chicago, Virginia, and others. Sunapee represented the smallest district in that cohort. When reviewing our situation with the cohort, it became very clear that no one felt that IT security was at a level to prevent this from happening in their district.

The State of New Hampshire receives federal monies under Title IV that are meant to help districts address providing technology for all, training and other creative initiatives. In New Hampshire, depending on the size and other aspects of a district, allocations can be between $10,000 and $30,000. Districts are required to propose projects for the expenditure of the funds and then must receive state approval before spending. While this sounds like a great support, unfortunately, only 15% of this grant can be spent on equipment or infrastructure. These allocations could be so much more beneficial to all districts if they could be used to invest in audits and to upgrade or enhance hardware to use cloud-based systems that would greatly improve IT data security in our schools.

Many school districts in New Hampshire have understaffed IT departments consisting of two or three full-time or part-time people. Given the rate that technology is changing and the amount of devices that are used to support education, they do not have the time to protect these systems as needed.

Thank you for asking me to speak with the Senate Subcommittee on Emerging Threats and Spending Oversight, and thank you to Senator Hassan for representing the state of New Hampshire by bringing this important topic to light.

Russell E. Holden
Sunapee Superintendent of Schools

70 Lower Main Street • Sunapee, NH 03782 • Tel: 603.763.4627 • Fax: 603.763.4718 • www.sunapeeschools.org

Hearing Before the Subcommittee on Emerging Threats and Spending Oversight
Homeland Security and Governmental Affairs Committee
U.S. Senate

"Addressing Emerging Cybersecurity Threats to State and Local Government"

June 17, 2021

Dan Lips
Vice President for National Security and Government Oversight, Lincoln Network

Chairman Hassan, Ranking Member Paul, and Members of the Subcommittee,
Thank you for the opportunity to testify.

My name is Dan Lips. I am the vice president for national security and government oversight at Lincoln Network, a non-profit organization focused on bridging gaps between the technology and policy communities.

As a former HSGAC staffer from 2011 to 2019, I'm sincerely honored to have the opportunity to testify today. I have a deep respect for the members and staff of the Committee and the important bipartisan work that is done in this hearing room.

My testimony focuses on policy and oversight options to help state, local, territorial, and tribal governments, and the private sector address growing cybersecurity threats.

We are all now aware that organizations across the United States are being targeted by ransomware attacks at an alarming rate. According to one recent estimate, U.S. organizations experienced 65,000 ransomware attacks in 2020.[1] At that rate, more than seven organizations will likely suffer a ransomware attack over the next hour.[2] The victims of these attacks include private sector and non-profit organizations, owners and operators of critical infrastructure, and governmental organizations (such as states, municipalities, school districts, and hospitals).

As the Committee will hear from the other panelists, ransomware attacks can stop organizations' operations while leaders make the difficult choice of whether to pay the ransom while working to unlock and restore information systems. Given attackers' economic incentives and the profitability of these kinds of attacks, we should expect ransomware to be an increasing problem moving forward. Beyond ransomware, organizations continue to face a broad range of cyber-attacks, such as nation-state sponsored economic and industrial espionage, traditional espionage, other financial crimes, and potential threats against critical infrastructure.

These threats require a proactive response by the federal government. But Congress should be thoughtful about the resources currently available to spend on cybersecurity as well as government agencies' capacity and track-record managing cyber responsibilities and grant

---

[1] David Gura, "U.S. Suffers Over 7 Ransomware Attacks An Hour. It's Now A National Security Risk," *NPR*, June 9, 2021.
[2] Ibid.

programs. According to Comptroller General Gene Dodaro, the United States is on an unsustainable fiscal path.[3] The Government Accountability Office (GAO) has warned that interest payments on the federal debt will exceed $1 trillion by 2033 and that the growing debt could bring a "large reduction in the value of the dollar" and limit Congress's ability to use fiscal policy to respond to future national emergencies.[4]

With this context, what should Congress, and specifically the Committee and Subcommittee, do to help states, localities, tribal, and territorial governments to manage growing cybersecurity risks?

I will offer four recommendations.

1. **Congress should streamline federal rules to reduce state governments' compliance costs to allow more state resources to be spent on improving security.**

For years, a top advocacy priority of the National Association of State Chief Information Officers ("NASCIO") has been for the federal government to "harmonize disparate federal cybersecurity regulations" and normalize the federal agency audit process.[5] For example, the Internal Revenue Service, Social Security Administration, and the Health and Human Services Department, among many others, have specific, and in some cases contradictory, rules for how to protect Americans' information. In 2020, GAO issued a report examining this problem and found that "the percentage of total requirements with conflicting parameters ranged from 49 percent to 79 percent."[6]

As a result, state officials spend much of their time on bureaucratic compliance. In 2018 testimony before the House Oversight Committee, the Oklahoma state CIO said that his office spent 10,712 hours on "compliance activities and support" that year, which amounted to five employees' entire year of work and nearly half of his team's time spent answering federal rules and audits.[7]

Streamlining federal rules would reduce the compliance burden imposed on state governments and free up time and resources currently devoted to compliance towards security. This would improve the cybersecurity posture of both state and local governments. In 2020, NASCIO and the National Governors Association issued a joint report describing how state governments were establishing initiatives to partner with localities to improve cybersecurity.[8]

---

[3] U.S. Government Accountability Office, GAO-21-275SP, *The Nation's Fiscal Health: After Pandemic Recovery, Focus Needed on Achieving Long-Term Fiscal Sustainability* (2021), https://www.gao.gov/products/gao-21-275sp.
[4] Ibid.
[5] "NASCIO Releases 2021 Federal Advocacy Priorities: Continues Call for Harmonized Cyber Regulations," NASCIO, January 14, 2021, at: https://www.gao.gov/products/gao-21-275sp.
[6] U.S. Government Accountability Office, *GAO-20-123, Cybersecurity: Select Federal Agencies Need to Coordinate on Requirements and Assessments of States* (2020), https://www.gao.gov/products/gao-20-123.
[7] James "Bo" Reese, "Regulatory Divergence: Failure of the Administrative State" Statement Before Oversight and Government Reform Committee, 2018.
[8] NGA and NASCIO, *Stronger Together: State and Local Cybersecurity Collaboration* (2020), https://www.nga.org/wp-content/uploads/2020/01/NASCIO_NGAStatesLocalCollaboration.pdf.

In the past, the National Governors Association has joined NASCIO in writing to the Office of Management and Budget (OMB) to ask the administration to address this problem of overlapping and contradictory federal information security rules.[9] Last May, GAO reported that OMB had issued guidance directing federal agencies to coordinate information security rules and compliance requirements, but had not required agencies to do so.[10] The Committee should pass legislation directing OMB to require agencies to harmonize information security rules to reduce the compliance burden on state governments.

2. **Congress should prioritize cybersecurity in existing homeland security grant programs and states should use currently available federal funds to close cybersecurity capability gaps.**

Simply streamlining the compliance burden alone will not close states and localities capability gaps to address current cyber threats. This will also require additional resources. I appreciate that there is interest in Congress and among members of the Committee to establish a new federal grant program for cybersecurity.

But the Department of Homeland Security, through the Federal Emergency Management Agency, already awards more than $1 billion annually to state and local partners to address homeland security needs including cybersecurity.[11]In the past, DHS has required states and localities to use 5 percent of their homeland security grant funds to improve cybersecurity capabilities. In February, Secretary Mayorkas stated that the Department would increase that requirement to 7.5 percent.[12] Congress, however, could require even larger percentages to be spent on cybersecurity. DHS's homeland security grants were expanded after the 2001 terrorist attacks to address existing counterterrorism and public safety capability gaps and buy-down risk. But past oversight by GAO and members of the Committee, including my former boss Senator Tom Coburn, have raised questions about the extent to which these funds have been used to measurably buy-down risk[13] or instead to subsidize routine public safety costs.[14] Given current threats, it would be appropriate for states and urban areas to use existing DHS grant funds to improve cybersecurity capabilities.

Importantly, states and localities do not need to wait for new grant awards to do this. They already have billions in unused homeland security grants that could be readily deployed to address current cyber threats this year. In 2020, OMB reported that states had not spent $2.7

---

[9] Letter to Mick Mulvaney, OMB Director, "Reducing Burdensome Cyber Regulations," NGA and NASCIO, November 6, 2017, at: https://www.nga.org/advocacy-communications/letters-nga/reducing-burdensome-cyber-regulations/.

[10] U.S. Government Accountability Office, GAO-20-123, *Cybersecurity: Select Federal Agencies Need to Coordinate on Requirements and Assessments of States* (2020), https://www.gao.gov/products/gao-20-123.

[11] "FY2021 Homeland Security Grant Program," Federal Emergency Management Agency, https://www.fema.gov/grants/preparedness/homeland-security.

[12] Benjamin Freed, "DHS announces $25M increase in cybersecurity grant funding," *State Scoop*, February 25, 2021.

[13] U.S. Government Accountability Office, GAO-18-354, Homeland Security Grant Program: Additional Actions Could Further Enhance FEMA's Risk-Based Grant Assessment Model (2018), https://www.gao.gov/products/gao-18-354.

[14] Senator Tom Coburn, *Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities* (2012), Homeland Security and Governmental Affairs Committee.

billion of the $5.3 billion that had been provided through the State Homeland Security Grant and the Urban Area Security programs between 2015 and 2020.[15] In other words, roughly 50 percent had not been spent. This means that at least $2 billion, and perhaps more, is likely still unspent and could be used today to address current cybersecurity capability gaps.

Also, states, localities, and even state education agencies and school districts should consider how other currently available federal resources could be spent to improve cybersecurity. For example, the American Rescue Plan is providing $350 billion to state, local, territorial, and tribal governments. According to the Treasury Department, Congress "provide[d] substantial flexibility" for governments to use these funds to meet local needs.[16] Moreover, Congress has provided an unprecedented infusion of federal emergency funds to state education agencies during the pandemic. But at least $180 billion of these emergency funds remained unspent as of this spring.[17] These funds should primarily be used to reopen schools and help disadvantaged children recover from prolonged school closures that occurred during the pandemic. However, state education agencies could use some of the available funding to improve cybersecurity defense to protect against ransomware attacks on schools and prevent future schooling disruptions, which could create additional setbacks for American children.

In short, state and local partners should use currently available resources to address current cybersecurity capability gaps before establishing new grant programs and awarding new funding. Congress and the Subcommittee should conduct oversight to determine what resources are currently available.

3. **The federal government should share meaningful threat information and security recommendations to help organizations manage cyber risks.**

Over the past decade, Congress has recognized the importance of improving information sharing about cyber threats and recommending best practices. Congress has passed bipartisan laws to establish federal programs and initiatives to facilitate information sharing. But nonpartisan oversight by GAO and the Inspector General have identified limitations and opportunities to improve DHS's information sharing programs.[18] Concerns have included the timeliness of information shared, limited participation by private sector partners, and over-classification, to name a few. Congress and the Committee should press agencies to answer open

---

[15] Dan Lips, "States and Cities Could Use Billions of Unspent DHS Grants to #Protect2020," *Lawfare*, February 28, 2020.

[16] "Coronavirus State and Local Recovery Funds," U.S. Department of the Treasury, https://home.treasury.gov/policy-issues/coronavirus/assistance-for-state-local-and-tribal-governments/state-and-local-fiscal-recovery-funds.

[17] Dan Lips, "$180 Billion of K-12 COVID Relief Funds Are Still Unspent," *Foundation for Research on Equal Opportunity*, May 19, 2021.

[18] U.S. Government Accountability Office, GAO-21-288, *High Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (2021); DHS Office of Inspector General, OIG-20-74, *DHS Made Limited Progress to Improve Information Sharing under the Cybersecurity Act in Calendar Years 2017 and 2018* (2020).

watchdog recommendations. In addition to sharing information about cyber threats, Congress should require federal agencies to share meaningful information with state and local governments about potential vulnerabilities in the information technology ecosystem to improve their technology acquisitions and strengthen supply chain risk management.

Beyond information sharing, Congress should also focus on ways to leverage the federal government's expertise to help state and local governments understand and implement best practices. For years, security experts have recommended that the National Institute of Standards and Technology (NIST) help organizations improve cybersecurity practices by prioritizing the security controls in the cybersecurity framework. The framework includes a checklist of more than 100 recommendations, which offer high-level guidance that may be difficult for smaller organizations to fully implement.[19] There is a growing consensus in the private sector that organizations must treat cybersecurity as an enterprise-wide risk management challenge.[20] Helping organization identify which security measures to prioritize will help with risk management.

Above all, the federal government can help organizations use available resources to appropriately manage risks by providing clear and focused security recommendations. For example, the Biden administration recently issued a memo to American companies with five specific recommendations to prevent and prepare for ransomware attacks.[21] President Joe Biden's May executive order also includes specific directions for improving information security at federal agencies, such as to "adopt multi-factor authentication and encryption for data at rest and in transit" within 180 days.[22] These directions provide valuable security recommendations for non-federal partners, including state and local authorities.

4. **Congress and the Subcommittee should conduct a strategic review of national cybersecurity threats and assess current and future resource needs to manage long-term cybersecurity risks.**

The recent attacks against state and local government agencies are only the latest serious cyber threats. For a quarter century, national leaders have warned that the United States faces increasing cyber threats jeopardizing American economic and national security. In 2018, the White House estimated that malicious cyber activity cost the United States economy between $57 billion and $109 billion in 2016.[23] Beyond these estimated economic costs, the United States has suffered significant breaches that have undermined national security, such as the 2015 OPM hack and the 2020 Solar Winds breach. Looking forward, the Intelligence Community recently forecast that technological innovations will likely result in increasing competition in the cyber

---

[19] "Cybersecurity Framework," National Institute of Standards and Technology, https://www.nist.gov/cyberframework/framework (June 16, 2021).
[20] National Association of Corporate Directors and Internet Security Alliance, *NACD Director's Handbook on Cyber-Risk Oversight* (2020), https://nacdonline.org/insights/publications.cfm?ItemNumber=67298.
[21] Amanda Macias and Christina Wilkie, "Business leaders must take urgent action to counter ransomware threat, White House warns in memo," *CNBC*, June 3, 2021.
[22] The White House, *Executive Order on Improving the Nation's Cybersecurity* (2021).
[23] White House, *The Council of Economic Advisers, The Cost of Malicious Cyber Activity to the U.S. Economy* (2018).

domain in the future.[24] Congress should anticipate that these problems will likely grow over time.

Given the scope of the challenge that the nation is facing, Congress and the Subcommittee should examine what resources are being spent on cybersecurity compared to other national security priorities as well as other areas of federal spending. President Biden proposed spending $9.4 billion on federal civilian agency cybersecurity programs in his recent budget request.[25] This represents a 14 percent increase above last year's funding.[26] In comparison, President Biden proposed spending $753 billion on the national defense budget.[27] Congress should review current and anticipated future security threats and consider whether these allocations of resources are appropriately balanced. Beyond national security funding, there are other areas of significant waste that that are much larger than what Congress spends on cybersecurity. For example, GAO estimates that the federal government made $175 billion in improper payments in FY2019, including approximately $75 billion reported as a monetary loss.[28]

Since members of the Committee are interested in establishing a new grant program to provide additional resources to state, local, tribal, and territorial governments for cybersecurity, it would be appropriate to identify potential areas of savings in the federal budget and opportunities to reallocate current government spending.

Conclusion

Once again, thank you for the opportunity to testify.

The Unites States faces serious security and fiscal challenges. State, local, tribal, and territorial governments are currently on the front lines facing growing cyber threats. Congress and the Biden administration have an opportunity to help them better manage cyber risks by streamlining federal rules to reduce compliance costs and by sharing useful threat information and security recommendations. For their part, state and local governments have an opportunity to use currently available funding, including more than $2 billion in unspent homeland security grants, to improve their cybersecurity capabilities. Looking forward, Congress and the Subcommittee should review current and anticipated security threats and long-term resource needs to manage cyber risks in the years ahead.

---

[24] Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community* (2021), p.20.
[25] The White House, *FY2022 Budget*, "Information Technology and Cybersecurity Funding," U.S. Defense Department, https://www.whitehouse.gov/wp-content/uploads/2021/05/ap_12_it_fy22.pdf.
[26] Ibid.
[27] "The Department of Defense Releases the President's Fiscal Year 2022 Defense Budget," May 28, 2021.
[28] US Government Accountability Office, GAO-20-344, *Payment Integrity: Federal Agencies' Estimates of FY 2019 Improper Payments*, (2020), https://www.gao.gov/products/gao-20-344.

AMERICAN PUBLIC GAS ASSOCIATION

June 30, 2021

The Honorable Maggie Hassan
Chairwoman, Emerging Threats and Spending Oversight Subcommittee, Senate Committee
on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Rand Paul
Ranking Member, Emerging Threats and Spending Oversight Subcommittee, Senate Committee
on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Re: June 17, 2021 Subcommittee Hearing on "Addressing Emerging Cybersecurity Threats to State and Local Government"

Dear Chairwoman Hassan and Ranking Member Paul:

The American Public Gas Association (APGA) writes regarding the Subcommittee's June 17, 2021 hearing on "Addressing Emerging Cybersecurity Threats to State and Local Government."

As Mayor Schewel mentioned in his testimony at the hearing, many municipal governments are responsible for operating systems that provide essential services like water and energy to their communities. Our members are those municipally owned service providers.

APGA is the trade association for approximately 1,000 communities across the U.S. that own and operate their retail natural gas distribution entities. Our members include municipal gas distribution systems, public utility districts, county districts, and other public agencies, all locally accountable to the citizens they serve. Public gas systems focus on providing clean, safe, reliable, and affordable energy to their customers and support their communities by delivering fuel to be used for cooking, clothes drying, and space and water heating, as well as for various commercial and industrial applications.

We appreciate the Subcommittee's attention to the unique challenges and needs of state and local governments when it comes to cybersecurity. As lawmakers consider what measures are needed to secure our nation's energy infrastructure and how to best support cybersecurity efforts at the state and local level, we urge you to remember that publicly owned natural gas systems face many of the same challenges and resource constraints that you heard about from witnesses at this hearing.

APGA's member utilities provide an essential service to their communities and are responsible for safeguarding their customers' personal and financial data, so they take their cybersecurity

responsibilities very seriously. Because they are community owned, however, public gas systems operate very differently than others in the natural gas value chain.

Our members often operate in rural areas or small towns, which means their distribution systems are correspondingly smaller. Unlike a large liquid transmission pipeline operator like Colonial, our members have few, if any, remotely controlled pipeline operations. This means they are less likely to employ operational technology (OT) assets. While there is a focus on protecting OT assets for those that have them, our members are more likely focused on protecting citizens' data within their information technology (IT) systems, just like the witnesses on your Subcommittee's panel.

Like any energy company, public natural gas utilities implement cybersecurity measures to mitigate risk to their systems and operations. Ensuring customer data and any IT or OT assets are secure is of paramount importance, but our members also face a very delicate balancing act when it comes to deciding to invest in new cybersecurity measures. APGA members work hard to commit resources to mitigate cybersecurity threats. However, unlike investor-owned utilities, public gas systems are not-for-profit entities and are dependent on a city council or local utility board for budget approval. Those operating budgets and rates are sometimes set years in advance with a focus on keeping energy as affordable as possible for their communities. As a result, our members must carefully weigh the benefits and costs of implementing new cybersecurity measures and can only make changes after discussions with and approval from local policymakers.

APGA appreciates the Chair's recognition of the budgetary challenges faced by state and local governments who may want to invest in cybersecurity but lack the resources or manpower to do so. We do believe that a dedicated grant program would be beneficial to help entities like our members adapt and comply as more guidance is issued at the federal level regarding how we should be hardening our systems against ransomware and other cyberattacks.

While additional federal funding for these efforts would certainly be useful, what is most important is that new federal legislation or regulations in the cybersecurity space be appropriately tailored. From our members' perspective, it is vital that lawmakers ensure that any new cybersecurity requirements are based on the results of thorough investigations into recent ransomware attacks against companies like Colonial and JBS. This will ensure that new measures adequately address current threats, but we are not faced with unnecessary "solutions" in search of a problem.

We also urge you and your fellow Committee members to ensure that the federal government is coordinated in its oversight efforts. APGA members have historically worked very well with the Transportation Security Administration (TSA). The resources and tools TSA provides have been vital to helping public natural gas utilities protect their assets. We are aware of legislative proposals that would potentially create additional cybersecurity oversight authority for energy infrastructure at other agencies. Duplicative or conflicting cybersecurity guidance and regulations will be especially burdensome for municipally owned utilities who do not have the resources or expertise to struggle through additional red tape. Local governments need clarity regarding federal agencies' roles in preparing for and recovering from cyberattacks in order to be as effective as possible.

Finally, we would echo testimony heard at the hearing regarding the importance of avoiding a one-size-fits-all approach to cybersecurity. Our members, like the cities and municipalities that control them, vary in size and access to resources. As has been discussed at length, our members also operate very differently from other energy companies because of their public ownership structure. Any new

cybersecurity mandates and any new federal grant program to support future investments should take these factors into account by providing flexibility and incorporating feedback from state and local stakeholders.

APGA applauds the Subcommittee's commitment to supporting its state and local government partners in the critical work of securing their data and assets against cyberattacks. We appreciate the opportunity to contribute the perspective of municipally owned natural gas utilities, and we hope to engage in further discussion as the Subcommittee considers a potential cybersecurity grant program.

Dave Schryver
President & CEO
American Public Gas Association
201 Massachusetts Avenue, NE, Suite C-4
Washington, DC 20002
dschryver@apga.org

○